GRC
GENDARMERIE ROYALE DU CANADA

Au service de la communauté policière depuis 1938

# GAZETTE

Vol. 70, N° 1, 2008
www.grc-rcmp.gc.ca

**LES OLYMPIQUES DE 2010**
La lutte aux fraudes concernant les Jeux

**FRAUDES DANS L'AIDE AUX VICTIMES**
Les leçons tirées de l'ouragan Katrina

**LE WIKI**
Le public collabore à la révision de la loi sur la police de Nouvelle-Zélande

## Mise au jour des escroqueries
### La répression de la fraude

Gendarmerie royale du Canada | Royal Canadian Mounted Police
Canada

# La fraude ne connaît pas de frontières

Dans tout ce qu'on lit ou entend à propos des arnaques et de la fraude, les détails sont parfois difficiles à croire : mesquinerie des criminels pour soutirer de l'argent ou crédulité du public malgré les avertissements. Le fait est que la fraude ne disparaîtra jamais complètement. D'où l'importance de lui faire obstacle.

Le présent numéro porte sur la fraude, plus précisément sur certains stratagèmes employés par les fraudeurs sans scrupules et les moyens les plus efficaces de lutter contre la fraude.

L'article-vedette traite des fraudes majeures par marketing de masse impliquant des faux chèques, effectuées depuis le Nigeria, ces opérations font des victimes un peu partout dans le monde. Les organismes d'application de la loi des États-Unis, du Canada, du Royaume-Uni, des Pays-Bas et du Nigeria participent conjointement aux enquêtes transfrontalières sur ces fraudes. Ce genre de partenariat international est maintenant la voie à suivre pour contrer la fraude et d'autres crimes.

Un autre article porte sur le rôle du Bureau national de lutte contre la contrefaçon de la GRC dans l'analyse et la reconnaissance de la fausse monnaie et des faux documents saisis lors d'enquêtes. Le Bureau a récemment modifié son mandat afin de fournir des conseils à des organismes non policiers, un rôle bien accueilli et nécessaire.

Dirigé par la GRC, le Groupe intégré de la sécurité (GIS) pour les Jeux olympiques et paralympiques d'hiver 2010 à Vancouver a été mis sur pied afin d'examiner les questions de sécurité complexes entourant cet événement international. En raison des coûts de construction estimés à plus de 3,1 milliards de dollars, le groupe spécial de renseignements financiers du GIS a été créé afin de protéger les fonds publics et privés liés à l'infrastructure des Jeux. Vous apprendrez en quoi cette approche gagnante peut aider à prévenir la corruption.

Nos collaborateurs présentent les nombreuses façons dont les citoyens se font arnaquer, parfois à leur insu, et comment la police traite ces dossiers.

L'insp. Barry Baxter de la Sous-direction des infractions commerciales explique la fraude en matière d'identité et comment nos renseignements personnels et financiers sont devenus de précieuses marchandises. Le gend. Lloyd Schoepp de la Section des infractions commerciales de la GRC à Calgary présente une initiative conjointe entre la police locale et les détaillants, qui vise à sensibiliser la population à la fraude sur les cartes de paiement appelée « écrémage ».

David R. Dugas, avocat pour le Middle District de la Louisiane, présente le Hurricane Katrina Fraud Task Force et explique la fraude massive parallèle aux mesures de secours qui ont fait suite à l'ouragan. Il explique également trois principes de base pour les enquêtes sur la fraude en matière de secours aux sinistrés. À lire absolument.

Pour sa part, Jeffrey Rosenthal, Ph.D., de l'Université de Toronto, explique en quoi les mathématiques ont aidé à conclure une enquête importante sur une fraude en matière de loterie en Ontario. Les résultats de ses calculs étaient difficilement réfutables.

La fraude transfrontalière est très répandue. De plus en plus, les victimes sont ciblées par des criminels de l'extérieur de leur pays. Ne manquez pas cet article sur un Australien en visite au Mali kidnappé pour une rançon, on y souligne les dangers réels du maraudage sur Internet et explique en quoi la collaboration internationale peut sauver des vies.

Olaolu Adegbite, de la Commission nigériane contre les délits économiques et financiers, expose les mesures prises pour lutter contre la fraude en matière de frais payables à l'avance au Nigeria, notamment l'intensification de la répression et la prédiction de l'évolution de ce crime.

Enfin, David Jones du Serious Fraud Office du Royaume-Uni explique en quoi ce bureau a besoin de la collaboration internationale pour résoudre nombre de ses dossiers, dont une enquête majeure sur une victime canadienne.

Vous trouverez également dans ce numéro une entrevue avec le premier psychologue affecté aux enquêtes criminelles, les stratégies d'adaptation de certains enquêteurs de la GRC responsables de la lutte contre l'exploitation des enfants, l'utilisation du Web par la police de Nouvelle-Zélande pour encourager le public à formuler la nouvelle loi sur le maintien de l'ordre, et bien d'autres sujets.

Nous espérons que vous aimerez ce premier numéro de 2008.

Katherine Aldred

**Du nouveau sur la fraude – bibliothèque du Collège canadien de police**
**www.cpc.gc.ca/library_f.htm**

**Livres**

*Cendrowski, Harry. The Handbook of Fraud Deterrence*, Hoboken (NJ, É.-U.), John Wiley & Sons. HV 6691 C33 2007

Debenham, David. *The Law of Fraud and the Forensic Investigator*, Toronto (Ont., Canada), Carwell. KE 8973 D35 2006

Pickett, K. H. Spencer. *Corporate Fraud: A Manager's Journey*, Mississauga (Ont., Canada), John Wiley & Sons Canada. HV 6691 P58 2007

Trainor, Brian. *Stop Fraud: A Veteran Police Investigator Shows You How*, Calgary (Alb., Canada), Red Deer Press. HV 6691 T68 2007

United States. *Department of Justice. Education and Training in Fraud and Forensic Accounting*, U.S. National Institute of Justice, Washington DC (É.-U.). HV 8079 .F7 N21 2007

Waite, Mélanie. *Personal Information and Scams Protection: A Canadian Practical Guide*, Ottawa (Ont., Canada), RCMP. HV 6685 C2 W133 2007

...suite à la page 25

# La fraude ne connaît pas de frontières

Dans tout ce qu'on lit ou entend à propos des arnaques et de la fraude, les détails sont parfois difficiles à croire : mesquinerie des criminels pour soutirer de l'argent ou crédulité du public malgré les avertissements. Le fait est que la fraude ne disparaîtra jamais complètement. D'où l'importance de lui faire obstacle.

Le présent numéro porte sur la fraude, plus précisément sur certains stratagèmes employés par les fraudeurs sans scrupules et les moyens les plus efficaces de lutter contre la fraude.

L'article-vedette traite des fraudes majeures par marketing de masse impliquant des faux chèques; effectuées depuis le Nigeria, ces opérations font des victimes un peu partout dans le monde. Les organismes d'application de la loi des États-Unis, du Canada, du Royaume-Uni, des Pays-Bas et du Nigeria participent conjointement aux enquêtes transfrontalières sur ces fraudes. Ce genre de partenariat international est maintenant la voie à suivre pour contrer la fraude et d'autres crimes.

Un autre article porte sur le rôle du Bureau national de lutte contre la contrefaçon de la GRC dans l'analyse et la reconnaissance de la fausse monnaie et des faux documents saisis lors d'enquêtes. Le Bureau a récemment modifié son mandat afin de fournir des conseils à des organismes non policiers, un rôle bien accueilli et nécessaire.

Dirigé par la GRC, le Groupe intégré de la sécurité (GIS) pour les Jeux olympiques et paralympiques d'hiver 2010 à Vancouver a été mis sur pied afin d'examiner les questions de sécurité complexes entourant cet événement international. En raison des coûts de construction estimés à plus de 3,1 milliards de dollars, le groupe spécial de renseignements financiers du GIS a été créé afin de protéger les fonds publics et privés liés à l'infrastructure des Jeux. Vous apprendrez en quoi cette approche gagnante peut aider à prévenir la corruption.

Nos collaborateurs présentent les nombreuses façons dont les citoyens se font arnaquer, parfois à leur insu, et comment la police traite ces dossiers.

L'insp. Barry Baxter de la Sous-direction des infractions commerciales explique la fraude en matière d'identité et comment nos renseignements personnels et financiers sont devenus de précieuses marchandises. Le gend. Lloyd Schoepp de la Section des infractions commerciales de la GRC à Calgary présente une initiative conjointe entre la police locale et les détaillants, qui vise à sensibiliser la population à la fraude sur les cartes de paiement appelée « écrémage ».

David R. Dugas, avocat pour le Middle District de la Louisiane, présente le Hurricane Katrina Fraud Task Force et explique la fraude massive parallèle aux mesures de secours qui ont fait suite à l'ouragan. Il explique également trois principes de base pour les enquêtes sur la fraude en matière de secours aux sinistrés. À lire absolument.

Pour sa part, Jeffrey Rosenthal, Ph.D., de l'Université de Toronto, explique en quoi les mathématiques ont aidé à conclure une enquête importante sur une fraude en matière de loterie en Ontario. Les résultats de ses calculs étaient difficilement réfutables.

La fraude transfrontalière est très répandue. De plus en plus, les victimes sont ciblées par des criminels de l'extérieur de leur pays. Ne manquez pas cet article sur un Australien en visite au Mali kidnappé pour une rançon; on y souligne les dangers réels du maraudage sur Internet et explique en quoi la collaboration internationale peut sauver des vies.

Olaolu Adegbite, de la Commission nigériane contre les délits économiques et financiers, expose les mesures prises pour lutter contre la fraude en matière de frais payables à l'avance au Nigeria, notamment l'intensification de la répression et la prédiction de l'évolution de ce crime.

Enfin, David Jones du Serious Fraud Office du Royaume-Uni explique en quoi ce bureau a besoin de la collaboration internationale pour résoudre nombre de ses dossiers, dont une enquête majeure sur une victime canadienne.

Vous trouverez également dans ce numéro une entrevue avec le premier psychologue affecté aux enquêtes criminelles, les stratégies d'adaptation de certains enquêteurs de la GRC responsables de la lutte contre l'exploitation des enfants, l'utilisation du Web par la police de Nouvelle-Zélande pour encourager le public à formuler la nouvelle loi sur le maintien de l'ordre, et bien d'autres sujets.

Nous espérons que vous aimerez ce premier numéro de 2008.

**Katherine Aldred**

**Du nouveau sur la fraude - bibliothèque du Collège canadien de police**
**www.cpc.gc.ca/library_f.htm**

United States. *Department of Justice. Education and Training in Fraud and Forensic Accounting*, U.S. National Institute of Justice, Washington DC (É.-U.). HV 8079 .F7 N21 2007

Waite, Mélanie. *Personal Information and Scams Protection: A Canadian Practical Guide*, Ottawa (Ont., Canada), RCMP. HV 6685 .C2 W133 2007

...suite à la page 26

# GAZETTE

Vol. 70, N° 1, 2008

Une publication de la Gendarmerie royale du Canada


## Dossier

### La fraude



## Rubriques



**EN COUVERTURE**

Nulle autre forme de criminalité ne semble stimuler la créativité des criminels comme la fraude. Mais qu'il s'agisse de l'arnaqueur qui cible ses victimes dans la sécurité perçue de leur foyer, dans des commerces locaux ou même par suite d'une catastrophe, les forces policières et leurs partenaires sont de plus en plus au fait des stratagèmes des fraudeurs, et unissent leurs efforts pour les réprimer.

**LA *GAZETTE* EN LIGNE A UN NOUVEAU SITE!**

**INSCRIVER**

***www.rcmp.ca/gazette/index.html/***

dans vos signets et venez faire un tour.


ÉDITRICE – Nancy Sample RÉDACTRICE EN CHEF – Katherine Aldred JOURNALISTE – Caroline Ross GRAPHISME – Jennifer Wale
ADMINISTRATION ET DIFFUSION – Angela Muia TRADUCTION – Services de traduction de la GRC IMPRIMERIE – Performance Printing





La *Gazette* (ISSN 1196-6513) est publiée en versions française et anglaise par la Direction des relations publiques et des services de communication de la Gendarmerie royale du Canada, à Ottawa. La conception de la page couverture ainsi que les articles sont protégés par les droits d'auteur et aucune partie de cette revue ne peut être reproduite sans consentement écrit. Poste-publication, numéro de convention 40064068. La *Gazette* paraît quatre (4) fois par année et est distribuée gratuitement mais en nombre restreint aux services de police et aux organismes d'exécution de la loi. On conseille fortement de la faire circuler. On ne peut pas s'y abonner à titre personnel. On vous prie de faire parvenir vos lettres, articles et commentaires à la Rédactrice en chef de la *Gazette*. La rédaction se réserve le droit de faire la révision. Pour communiquer avec nous : La rédactrice en chef — la *Gazette* de la GRC, immeuble L.H. Nicholson, pièce A200, promenade Vanier, Ottawa (Ontario) CANADA K1A 0R2, par téléphone : (613) 998-6307, par télécopieur : (613) 993-3098, par courriel : gazette@grc-rcmp.gc.ca, par Internet : ***www.rcmp.ca/gazette/index.html***

## INAUGURATION DU CENTRE D'ACCUEIL DES VISITEURS ÉTRANGERS DE LA GRC

Les visiteurs étrangers à la Direction générale de la GRC à Ottawa disposent désormais d'un endroit pour rencontrer le personnel de la GRC, tenir des réunions et se détendre entre deux rendez-vous.

Le Centre d'accueil des visiteurs étrangers, inauguré officiellement le 28 septembre 2007, est le centre de liaison pour les délégations en visite à Ottawa, explique le s.é.-m. Pierre Patenaude, ancien gestionnaire (aujourd'hui retraité) de la Sous-direction des visites et des voyages internationaux de la GRC. Toutes les rencontres s'y dérouleront.

On y trouve une salle de réunion de 25 places, l'accès à Internet et des installations de téléconférence, le tout à proximité de l'entrée principale de la Direction générale. Un coin salon permet aux visiteurs de se détendre en toute sécurité entre deux rendez-vous.

« Les gens auront un lieu pour prendre un café ou un thé, et discuter entre eux ou avec des membres de la GRC », ajoute le s.é.-m Patenaude.

Le Centre est la dernière addition au Programme du protocole et des visites internationales, qui a été mis sur pied en 2003 et offre aux délégations toute une gamme de services : accueil à l'aéroport, transport à bord de véhicules de la GRC, itinéraires adaptés et divers autres services organisés par un agent des visites protocolaires.

Le s.é.-m. Patenaude précise que le programme est très populaire auprès des visiteurs et qu'il favorise les relations internationales. De fait, les agents de liaison de la GRC à l'étranger ont élargi leurs contacts depuis l'établissement du programme; la GRC est à même de mieux collaborer avec ses partenaires étrangers à des enquêtes transfrontières.

Caroline Ross

Le comm. William J. S. Elliott coupe le ruban pour inaugurer le nouveau Centre d'accueil des visiteurs étrangers, en présence de Raf Souccar, comm. adj. aux Opérations fédérales et internationales.

Depuis 2003, la Direction générale de la GRC a accueilli 1393 visiteurs de 404 délégations. La plupart des visiteurs proviennent de Chine, des États-Unis et d'Afrique du Sud.

*—Caroline Ross*

## DES ÉQUIPES CHARGÉES DE LUTTER CONTRE LA CORRUPTION INTERNATIONALE

La lutte contre la corruption internationale doit être menée à l'échelle mondiale. D'ici avril 2008, deux nouvelles équipes de la GRC y participeront.

Les deux équipes, dont les bureaux seront à Ottawa et à Calgary, concentreront leurs efforts sur la détection de la corruption internationale (corruption, blanchiment d'argent, détournement de fonds, etc.) ainsi que les enquêtes et la prévention en la matière. La mise sur pied des équipes aidera le Canada à remplir les engagements qu'il a pris dans le cadre de la Convention des Nations Unies contre la corruption (CNUCC).

« La lutte contre la corruption internationale passe par la volonté des États de collaborer pour établir des règles du jeu équitables », déclare le surint. Stephen Foster, directeur de la Sous-direction des délits commerciaux de la GRC dont les deux équipes feront partie.

La CNUCC prévoit plusieurs mesures qui visent à améliorer la coopération internationale dans la lutte contre la corruption, dont l'exigence pour chacun des pays signataires d'avoir un organe de prévention de la corruption, de l'application des politiques anticorruption, de l'accroissement et de la diffusion des connaissances ainsi que du soutien aux partenaires étrangers dans la lutte anticorruption.

Le Canada répondra à ce critère grâce aux équipes de la GRC qui cibleront tout particulièrement la corruption dans le secteur public, et donc la corruption d'agents publics canadiens et étrangers et le blanchiment des produits de la criminalité qui en découle.

« Les équipes auront pour mission de recueillir des renseignements, d'établir des contacts et d'identifier les cibles tactiques pour les enquêtes », précise le surint. Foster. Il ajoute que les enquêteurs spécialisés dans la lutte contre la corruption sont importants, car ils permettent aux organismes d'application de la loi de mener des enquêtes approfondies dans les cas de corruption, sans pour autant amoindrir les ressources affectées à d'autres enquêtes en cours.

Les équipes de la GRC travailleront en étroite collaboration avec des organismes d'application de la loi étrangers ainsi qu'avec des partenaires canadiens comme le ministère des Affaires étrangères et du Commerce international (MAECI) et le ministère de la Justice, qui participent tous deux, pour le compte du gouvernement du Canada, à la mise en oeuvre des autres exigences de la Convention.

La CNUCC est le premier instrument international juridiquement contraignant contre la corruption. La Convention est entrée en vigueur en décembre 2005 et a été ratifiée par plus de 100 pays membres, dont le Canada, en octobre 2007.

Outre l'application de la loi, la CNUCC vise l'amélioration de la responsabilisation dans les secteurs public et privé et l'accélération des poursuites relatives à la corruption.

*—Caroline Ross*

## LA TECHNOLOGIE POLICIÈRE AU SERVICE DES FORCES MILITAIRES

Les forces militaires canadiennes évaluent présentement un système d'établissement de profils géographiques mis au point par la police canadienne pour faciliter le repérage et l'arrestation de criminels en série en vue de son usage dans le cadre d'activités anti-insurrectionnelles outre-mer.

Élaboré par Kim Rossmo, ancien policier de Vancouver, au milieu des années 90, le système permet aux utilisateurs d'entrer les coordonnées géographiques de lieux de meurtres, de viols, de vols qualifiés ou d'autres crimes en série et d'obtenir une carte indiquant les secteurs où il est le plus probable que leur auteur habite, d'après les endroits où les crimes ont été commis.

« Il s'agit simplement d'appliquer la loi du moindre effort », affirme Ian Laverty, président et premier dirigeant d'Environmental Criminology Research Inc. (ECRI), la compagnie canadienne qui produit et distribue le logiciel de profilage géographique. « Le lieu de résidence le plus probable est celui à partir duquel il est le plus facile de se rendre à tous les lieux de crime. »

Recherche et développement pour la défense Canada (RDDC) collabore maintenant avec ECRI et d'autres partenaires pour déterminer si le système peut aider à combattre les attentats aux engins explosifs artisanaux (EEA) et à détecter les menaces.

« Nous essayons d'adapter cet outil policier aux besoins militaires. Ainsi, au lieu de réagir aux EEA, nous pourrons passer à l'offensive », précise le major Dave Waller, directeur du projet de protection contre les EEA du Programme de démonstration de technologies (PDT) de RDDC.

Le projet en est à ses débuts, mais le major Waller estime que le savoir policier jouera un rôle clé dans les futurs travaux de recherche et développement. En partenariat avec ECRI, Carl Sesely, auteur de profils géographiques à la GRC, gère le programme de formation logicielle à RDDC, mettant à profit ses sept ans d'expérience en profilage policier pour enseigner les théories fondamentales de la géographie du crime.

« La participation de tels experts a grandement favorisé l'acceptation de la capacité [de cet outil au sein des forces militaires] », croit le major Waller. Il ajoute que de nombreux principes du profilage géographique peuvent s'appliquer aux activités tant policières que militaires.

Sergt Jerry Kean, MDN

Un système de profilage géographique conçu pour la police pourrait aider les militaires canadiens à contrer la menace des attentats aux EEA, comme celui-ci, survenu en Afghanistan en 2005.

À l'heure actuelle, 82 services de police en Amérique du Nord et en Europe utilisent le logiciel de profilage géographique d'ECRI.

Pour en savoir davantage sur le logiciel d'ECRI, consultez le ***www.ecricanada.com***.

***—Caroline Ross***

## VENIR EN AIDE AUX VICTIMES D'INTIMIDATION

Selon des chercheurs canadiens, un enfant est victime d'intimidation à l'école à toutes les cinq minutes au Canada. Cependant, l'intimidation passe souvent sous silence parce que ceux qui en sont témoins ont peur d'intervenir et parce que les victimes se sentent seules et démunies.

« On ne tient jamais vraiment compte de ce que ressent la victime », de dire Jordan Boudreau, un élève de 9e année, qui décrit les programmes de lutte contre l'intimidation offerts par les écoles de la Nouvelle-Écosse (N.-É.), où il vit. « Si nous pouvons donner des moyens d'action aux victimes d'intimidation, nous n'aurons plus à nous préoccuper de ce problème, pas vrai? »

C'est exactement le message qu'a fait passer un mouvement étudiant de lutte contre l'intimidation en Nouvelle-Écosse l'automne dernier, mouvement qui a suscité l'attention des médias partout en Amérique du Nord et qui a gagné l'appui de la police provinciale.

Il a commencé lorsque deux élèves du secondaire ont vu un plus jeune se faire malmener parce qu'il portait une chemise rose à l'école. Le lendemain, ils sont arrivés à l'école vêtus d'une chemise rose et ont encouragé les autres à faire de même. Le message s'est répandu, au point où les écoles de la province ont tenu des « journées chemise rose » et que le premier ministre de N.-É. a fait du deuxième jeudi de la rentrée scolaire la « Journée contre l'intimidation ».

Les agents de liaison de la GRC qui travaillent dans les écoles à Halifax (N.-É.) portent maintenant un brassard rose pour montrer qu'ils appuient l'initiative des étudiants.

« Cette initiative est l'oeuvre d'étudiants et nous l'appuyons », précise le gend. Curt Wentzell, l'agent de la GRC à Halifax à l'origine du programme de brassards roses. « Les jeunes sont enthousiastes. Ils sont heureux de voir que des symboles d'autorité appuient leur initiative. »

Selon Wentzell, la lutte contre l'intimidation à l'école peut avoir des avantages à plus long terme, comme de réduire les actes d'intimidation dans les sports, le milieu de travail et ailleurs. « L'intimidation crée une spirale de violence qui s'apparente à la violence familiale », ajoute-t-il.

Treize policiers de la GRC se rendent régulièrement dans les écoles de la région d'Halifax; ils patrouillent les corridors et parlent aux jeunes d'intimidation, de drogues et de sécurité Internet.

***—Caroline Ross***

Des policiers de la GRC à Halifax (Nouvelle-Écosse) portent des brassards roses pour manifester leur appui envers une initiative de lutte contre l'intimidation lancée par des étudiants.

*Gend. Anna Cochrane, District d'Halifax*

# Se glisser dans la tête d'un criminel

## L'expérience d'un psychologue affecté aux enquêtes criminelles

*Il a pénétré le psychisme d'innombrables psychopathes, pédophiles ou preneurs d'otages. Il a passé de nombreuses heures dans le système carcéral à évaluer des prédateurs sexuels. Il est l'une des 17 personnes en Amérique du Nord à être à la fois policier et psychologue et, chose plus rare encore, il est l'un l'un de ceux qui sont spécialisés dans l'étude du comportement criminel. Le sergent d'état-major Matt Logan, premier psychologue de la GRC affecté aux enquêtes criminelles, parle de son travail à Caroline Ross, de* la Gazette.

**Dans votre carrière, quel a été le cas le plus marquant?**

Celui qui a été le plus traumatisant, c'est lorsqu'un preneur d'otages a tué un otage sous mes yeux. J'étais le négociateur. C'était en 1988, lors de ma première négociation. Cela n'a pas été un bon début pour moi, mais cela m'a poussé à commencer ma maîtrise en psychologie à l'Université de Victoria. J'ai compris que l'individu était un psychotique et que je n'avais aucune idée de ce qui se passait dans sa tête. Faute de connaissances, je me suis senti complètement impuissant.

**Comment êtes-vous arrivé au poste de psychologue affecté aux enquêtes criminelles?**

Après avoir obtenu ma maîtrise, j'ai été affecté à Ottawa pour trois ans. Les membres de l'EMS (l'État-major supérieur de la GRC) de l'époque, après l'épisode de Gustafson Lake, se sont demandé : « N'avons-nous personne à la GRC qui possède un diplôme d'études supérieures en psychologie et qui puisse nous aider à faire face à un autre incident majeur comme celui de Gustafson Lake? »* . Ils s'imaginaient alors que ce genre de situation de crise se produirait souvent. Ils m'ont demandé si j'étais prêt à faire un doctorat et j'ai accepté.

**Quel est votre rôle principal à la GRC?**

En fait, mon rôle est multiple. Selon les cas, je peux être assistant ou consultant. En ce moment, je travaille surtout sur des crimes graves. L'une de mes fonctions est de me pencher sur les affaires non résolues. Examiner les personnes d'intérêt et déterminer lequel des suspects est probablement le coupable, selon le psychisme de l'individu et les diverses facettes de sa personnalité.

À titre de psychologue affecté aux enquêtes criminelles à la GRC, le s.é.-m. Matt Logan est entre autres chargé de déceler les points faibles affectifs, les troubles mentaux ou la passivité des individus interrogés.

Caroline Ross

**Sur quels facteurs reposent vos évaluations?**

Lorsque nous savons que nous avons affaire à un psychotique, par exemple (la psychopathie est déterminée par un processus de diagnostic pour lequel les psychologues ont reçu une formation), nous pouvons tirer des conclusions des traits de personnalité, du niveau de violence ou de la gratuité de cette violence. Nous pouvons ensuite examiner les circonstances du crime : Comment a-t-il été commis? Quand? Dans quel contexte? Nous pouvons alors évaluer la possibilité que le crime ait été perpétré par un psychotique.

**Vous travaillez beaucoup avec des équipes d'interrogateurs. Quel est alors votre rôle?**

Je m'assois dans une pièce où je peux suivre l'interrogatoire en direct et j'observe. Cela me permet de conseiller les interrogateurs. Je leur dis ce que je vois de l'état d'esprit de l'individu, de sa constitution psychologique et de ses points faibles affectifs que nous pouvons utiliser pour développer une relation plus forte avec lui. Je peux aussi leur parler de la relation qui s'établit avec lui ou de ce qui peut manquer pour qu'elle se consolide. Je guette également les signes de passivité, pour être sûr que nous n'enregistrons pas de faux aveux.

**Pendant deux ans, vous avez fait de la thérapie auprès de prédateurs sexuels dans le système carcéral de la Colombie-Britannique. Qu'en avez-vous retenu?**

J'ai beaucoup appris sur les délinquants, sur leur mentalité et leurs besoins. La connaissance du délinquant qui est en face de vous se révèle le plus souvent d'une grande utilité. Dans le cas des opérations d'infiltration, il est particulièrement important que nous connaissions les besoins de la cible. Est-ce le pouvoir? l'ego? la cupidité? Voilà les trois motivations principales. Si vous me dites que son premier motif est l'argent, son deuxième, le pouvoir et son troisième, l'ego, je serai alors en mesure de vous guider dans votre travail d'infiltration. ■

** En 1995, l'échec des négociations pour mettre un terme à l'occupation des terres à Gustafson Lake (C.-B.) a donné lieu à l'un des plus grands déploiements de forces policières de l'histoire du Canada.*

# COMBATTRE LES ARNAQUES AUX CHÈQUES FRAUDULEUX

## Les partenaires internationaux se passent le mot


Par Caroline Ross

**Un homme d'affaires au Royaume-Uni vous envoie un courriel disant qu'il souhaite louer le logement que vous avez annoncé en ligne. Il vous poste un chèque d'entreprise pour 12 mois de loyer. Vous le déposez, puis vous recevez un autre courriel : la mutation est tombée à l'eau. Pouvez-vous retourner le dépôt par virement télégraphique, moins un petit dédommagement?**

Vous acceptez sans jamais vous douter que l'« homme d'affaires » est un jeune Nigérian dans un café Internet, que le « chèque d'entreprise » est un faux posté au Canada et que les fonds envoyés par virement télégraphique ont été encaissés par des associés criminels à Singapour.

Tout ce que vous savez – lorsque votre banque vous appelle un mois plus tard pour vous signaler que le chèque était contrefait – c'est que vous devez rembourser les pertes. Vous n'êtes qu'une autre victime de fraude en marketing de masse commise à l'aide de faux chèques.

Arnaques liées à une location, à une loterie, à un paiement excédentaire, à un héritage – la liste est sans fin. Et c'est un domaine payant. De janvier à octobre 2007, les autorités policières des États-Unis, du Canada, du Royaume-Uni, du Nigeria et des Pays-Bas ont saisi des instruments financiers contrefaits dont la valeur nominale totalisait plus de 2,1 milliards de dollars.

« C'est un problème mondial », confirme l'insp. Mario Beaulne, responsable des Fraudes majeures à la GRC. « Un monsieur en Finlande reçoit une lettre de Singapour et doit envoyer de l'argent au Canada. Où sont les bandits? Ils sont partout. »

Les fraudeurs utilisent les frontières internationales et Internet pour brouiller les cartes, mais les forces de l'ordre leur dament le pion petit à petit, remontant la piste des courriels, des lettres et des virements de fonds transfrontaliers, établissant des liens et appréhendant des suspects.

## Dépister les communications sur Internet

« La plupart des victimes, où qu'elles se trouvent, sont ciblées par Internet », dit Greg Campbell, inspecteur responsable de la sécurité et des enquêtes mondiales au sein du U.S. Postal Inspection Service (USPIS).

Ce sont aussi majoritairement des citoyens américains, réalité qui découle en partie du droit bancaire des États-Unis qui oblige les banques à rendre disponibles en cinq jours les fonds déposés, même si la compensation d'un chèque peut prendre des semaines, voire des mois.

Pour composer avec ce problème, les enquêteurs du USPIS ont interviewé des victimes de fraude et dressé la liste des adresses courriel touchées. En collaborant étroitement avec des fournisseurs de services Internet du secteur privé, ils ont réussi à remonter la piste des communications jusqu'aux adresses IP initiales.

Greg Campbell, Service d'inspection postale des É.-U.

Des agents américains et nigérians ont découvert plusieurs chèques contrefaits dissimulés dans des tongs, que les fraudeurs nigérians prévoyaient envoyer par courrier à des complices à l'étranger.

Comme la plupart de ces adresses relevaient du Nigeria, explique l'insp. Campbell, le USPIS a collaboré avec l'Economic and Financial Crimes Commission de ce pays pour tirer profit des renseignements recueillis sur place. Le partenariat s'est avéré si efficace que les collaborateurs ont pu cibler des cybercafés déterminés et arrêter plusieurs fraudeurs sur-le-champ.

« Nous avons utilisé les outils des suspects pour les trouver et les arrêter, précise l'insp. Campbell. C'était une collaboration entre le secteur privé et les autorités policières internationales, une première pour les États-Unis en matière de fraude. »

## Surveiller la poste

Les adeptes de la fraude en marketing de masse comptent également sur le système postal pour dissimuler leurs activités. Souvent, les faux chèques sont produits dans un pays, postés en vrac à des associés dans d'autres pays, puis repostés individuellement à des victimes à l'étranger.

Montréal figure parmi les nombreuses plaques tournantes du repostage, notamment dans le cadre de loteries frauduleuses visant des Américains, précise le serg. Yves Leblanc de la GRC.

Ce dernier y dirige le Projet COLT, l'une de six équipes canado-américaines qui enquêtent sur la fraude en marketing de masse basée au Canada. Les partenaires du projet, soit la GRC, la Sûreté du Québec, le Service de police de la Ville de Montréal, le FBI, les Services de sécurité et d'enquête de Postes Canada, le USPIS, l'Agence des services frontaliers du Canada, le U.S. Immigration and Customs Enforcement Bureau, la U.S. Federal Trade Commission et le Bureau de la concurrence du Canada, gèrent un programme qui permet de repérer et d'intercepter les faux instruments financiers qui entrent au Canada ou en sortent par la poste ou par messagerie.

Les partenaires savent quoi chercher, dit le serg. Leblanc. Les adresses au Nigeria, les effets négociables de plus de 10 000 $ et les paquets de lettres à taux d'affranchissement précis déposés dans des boîtes aux lettres publiques ne sont que quelques-uns des signes qui peuvent donner lieu à une enquête plus poussée afin de démasquer des fraudeurs.

« Lorsqu'on enquête sur ces fraudes, dit le serg. Leblanc, on découvre de petites cel-

lules de deux ou trois personnes, établies un peu partout, qui entretiennent souvent des relations au Nigeria. »

Si bon nombre des faux interceptés grâce au Projet COLT viennent du Nigeria, d'autres sont produits au Canada par des associés criminels. Cette tendance n'est devenue évidente qu'à la lumière des interceptions effectuées au cours des dernières années, précise le serg. Leblanc.

« C'est un travail difficile, mais très fructueux. Dans bien des cas, nous portons des accusations au Canada, et dans nombre d'autres, nous extradons les suspects aux États-Unis. »

## Suivre l'argent

En mars 2007, le Groupe d'analyse des renseignements criminels (GARC) du Centre d'appel antifraude du Canada (CAAC) a lancé un projet pilote d'un mois afin de suivre l'argent faisant l'objet de fraude transfrontalière par faux chèques, ce qui a permis d'autres constats.

Le CAAC est le dépôt des plaintes de fraude en marketing de masse au Canada. Le GARC analyse ces plaintes afin de dégager des tendances et de compiler des dossiers de renseignements.

« En étudiant les données recueillies pendant un mois, nous avons constaté que dans la vaste majorité des cas, les fraudeurs demandaient aux victimes d'envoyer de l'argent à des institutions financières étrangères », note le cap. Louis Robertson, l'agent de la GRC responsable du GARC.

La tendance était si marquée que le GARC a prolongé le projet pilote de façon indéterminée. Or, précise le cap. Robertson, c'est seulement six mois plus tard que les enquêteurs canadiens ont pu établir des liens avec d'autres fraudes internationales, lorsqu'ils ont rencontré leurs homologues américains, britanniques, nigérians et hollandais dans le cadre d'un plus vaste projet visant à évaluer conjointement la menace mondiale de la fraude en marketing de masse.

Cette réunion a clarifié la situation globale de la fraude transfrontalière par faux chèques.

« Chaque pays détient une partie de l'information, reconnaît l'insp. Beaulne. Une arnaque peut commencer au Nigeria, puis passer par des cellules ou des relations dans d'autres pays, comme le Canada ou les États-Unis. Au Canada, nous voyions les adresses des destinataires et les endroits où les victimes devaient envoyer leur argent, mais nous ne savions pas nécessairement qui s'occupait de poster les lettres. De leur côté, les autorités du Nigeria et des États-Unis (où des enquêteurs ciblaient les fraudeurs) ne savaient peut-être pas exactement où l'argent s'en allait. »

« La percée décisive est vraiment survenue lorsque tous les intervenants des différents pays ont pu mettre en commun leur information et cerner l'ensemble du processus. »

Ce processus n'est qu'un aspect d'un vaste réseau de fraude impliquant de nombreux autres pays et éléments. Les crimes se poursuivront tant que leurs auteurs trouveront de nouveaux endroits où exercer leurs activités ou adopteront de nouvelles tactiques pour en retarder la détection.

« Nous ne pouvons pas les arrêter tous, résume l'insp. Campbell du USPIS. Lorsque nous appréhendons un suspect, plein d'autres sont prêts à prendre sa place. Mais nous ne baisserons pas les bras. Nous continuerons d'enquêter sur ces crimes. »

Au fil des enquêtes et des échanges de renseignements, les autorités policières internationales font la lumière sur les voies empruntées par les criminels, leur laissant de moins en moins de cachettes. ■

Opération conjuguée du projet COLT à Montréal, a permis d'intercepter 14 646 lettres de loterie frauduleuse – et des chèques contrefaits d'une valeur de 46 millions $ – destinés à des victimes au Canada et aux États-Unis en novembre et en décembre 2007.


Projet COLT

## Sensibiliser le public

Repérer et poursuivre les escrocs, c'est un aspect de la lutte contre les arnaques internationales aux faux chèques. Apprendre au public comment reconnaître, signaler et éviter ces combines en est un autre.

« L'éducation est fondamentale, dans tous les pays, estime Greg Campbell, du USPIS. En apprenant aux gens comment éviter de devenir victimes, nous empêchons le crime. »

En octobre 2007, le USPIS et l'Alliance for Consumer Fraud Awareness des États-Unis ont lancé le ***www.fakechecks.org***, un site Web de sensibilisation du public consacré à la fraude par faux chèques au moyen d'Internet. On y trouve des vidéos, une foire aux questions et des entrevues avec des victimes qui aident les gens à reconnaître des arnaques courantes et à surmonter la honte associée au fait d'en être victimes.

Consultez le ***www.fakechecks.org***.

# Le Bureau national de lutte contre la contrefaçon

## Première défense de l'intégrité des documents canadiens

**Par Caroline Ross**

Quoi de neuf au Bureau national de lutte contre la contrefaçon (BNLC) de la GRC? Commençons par le mot national.

En août 2007, le Bureau est officiellement devenu un « centre d'expertise » en matière de lutte contre la contrefaçon et de sécurité des documents au Canada – un rôle qui aide à promouvoir la constance et l'unité dans les efforts nationaux de lutte contre la contrefaçon.

La GRC a commencé à examiner des documents suspects en 1937 et s'est dotée d'un groupe distinct d'analyse de la fausse monnaie en 1961. En 2003, les deux fonctions ont fusionné, devenant le Bureau d'expertise des contrefaçons et des documents, mais son mandat de soutien au travail des policiers ne reflétait pas le rôle qu'il remplissait de plus en plus, soit de conseiller les organismes gouvernementaux extérieurs au milieu policier.

« De par la nature de notre travail, nous connaissons une panoplie de méthodes utilisées pour contrefaire les éléments de sécurité des documents, qu'il s'agisse de monnaie, de passeports ou de permis de conduire, indique Shawki Elias, gestionnaire du BNLC. Nous savons quels éléments de sécurité sont menacés, et quelles sont ces menaces. »

Entre 2003 et 2006, le BNLC a analysé plus de 1,8 million de billets contrefaits et 30 000 documents suspects. Le Bureau examine chaque contrefaçon saisie au Canada, détermine quels sont les éléments vulnérables et suit l'évolution des tendances à l'aide d'une base de données. Le personnel du BNLC visite aussi les ateliers de contrefaçon démantelés, afin d'observer les outils et les techniques qu'utilisent les criminels.

Étant donné l'expérience acquise, résume Elias, le Bureau reçoit régulièrement des demandes d'aide d'organismes fédéraux et provinciaux pour protéger leurs documents de la contrefaçon.

« Pour déjouer les contrefacteurs, personne ne connaît mieux la fonctionnalité de nos documents et leur performance que l'équipe du BNLC, avoue d'emblée Andy Ward de la Banque du Canada. Aux analyses techniques et scientifiques de nos experts maison, ils ajoutent une dose de données factuelles précieuses. »

Ward est le gestionnaire du projet chargé de concevoir la prochaine génération de billets canadiens, dont la mise en circulation est prévue pour la fin de 2011. Il a invité Paul Laurin, du BNLC, à se joindre au groupe de travail parce que, selon lui, les gens du BNLC « ont une connaissance personnelle approfondie de la contrefaçon » et savent comment, dans le temps, les billets ont pu résister à la contrefaçon.

Cette perspective s'est déjà révélée utile, reconnaît Ward. Lors d'un débat sur la possibilité de modifier un élément de sécurité d'un billet particulier, Laurin s'est fié aux analyses du BNLC pour confirmer que l'élément était durable et copié de piètre façon par les faussaires.

« Cette expertise aide la Banque à prendre des décisions éclairées, » affirme Ward.

Le BNLC offre des conseils de même nature aux organismes responsables des documents d'identité, comme le passeport canadien, le certificat du statut d'Indien et les certificats de naissance provinciaux.

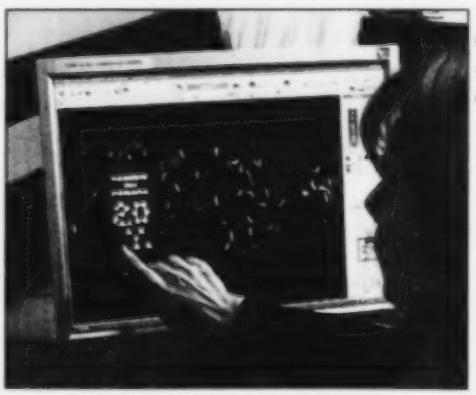
Le Bureau participe aussi à des initiatives gouvernementales, comme le groupe de travail interministériel sur l'intégrité des documents que dirige l'Agence des services frontaliers du Canada. Le BNLC y dirige les travaux du sous-groupe d'experts judiciaires chargé de recommander les éléments de sécurité minimums et d'analyser les prototypes de documents d'identité fédéraux et provinciaux.

Le sous-groupe a aidé le ministère des Transports de l'Ontario à intégrer au nouveau permis de conduire des éléments de sécurité d'avant-garde, comme la photo gravée au laser, qui le protègent mieux contre la manipulation.

« Rien ne vaut la connaissance de première main de ce qui se passe réellement, déclare Steve Burnett, gestionnaire du projet du permis de conduire de l'Ontario. Avec tous les vols d'identité et toute la contrefaçon dont on entend parler, nous avons le devoir de fournir aux Ontariens un document sûr qui protégera leur identité. »

Les efforts collectifs contribuent à normaliser l'intégrité des documents canadiens et favorisent des initiatives qui se soutiennent l'une l'autre. Par exemple, le demandeur d'un passeport peut produire un permis de conduire pour confirmer son identité. Si l'on réduit le nombre de permis de conduire contrefaits en circulation, le passeport canadien est à son tour mieux protégé.

Par le passé, conclut Elias, la concertation était défaillante au Canada en matière de protection de l'intégrité des documents. Ce n'est plus le cas aujourd'hui, et le BNLC n'y est pas étranger. ■



Caroline Ross

Sonia Michaud, spécialiste judiciaire au BNLC, utilise l'équipement spécialisé pour examiner par éclairage ultraviolet certains éléments de sécurité d'un billet de 20 $ canadien.

# Bâtir un héritage olympique

## Un groupe s'attaque à la fraude en matière de construction en prévision de Vancouver 2010

**Par Caroline Ross**

Neuf lieux de compétition, deux villages des athlètes, de grandes améliorations routières et de nouvelles lignes ferroviaires urbaines. Coût total prévu : plus de 3,1 milliards de dollars, provenant en grande partie des fonds publics.

Le développement de l'infrastructure en vue de la tenue des Jeux olympiques et paralympiques d'hiver 2010 à Vancouver, en Colombie-Britannique, est une entreprise lucrative mais pas toujours pour les sociétés de construction et les collectivités. Les fraudeurs et les groupes du crime organisé peuvent aussi se frotter les mains avec avidité.

Les rumeurs de corruption ont certainement occulté les Jeux de Montréal en 1976. Les fausses factures et les entrepreneurs sans scrupules auraient contribué à l'immense déficit de 3 G$ dont les contribuables ont mis 30 ans à venir à bout. Le budget initial était de 300 M$.

Pour éviter qu'une corruption similaire ne mine l'héritage olympique de Vancouver, le Groupe intégré de la sécurité (GIS) créé par la GRC pour les Jeux de Vancouver 2010 a formé un groupe spécial des renseignements financiers chargé de prévenir la fraude et de protéger les fonds publics (et privés) liés à la construction des Jeux.

« Nous fournissons un certain niveau de renseignements sur l'intégrité économique venant en fait appuyer environ 4,5 milliards de dollars en développement de l'infrastructure », affirme l'insp. Alex Graham, off. resp. du Groupe mixte de renseignements (GMR) du GIS, de qui relève le groupe de renseignements financiers.

Créé en mai 2005, le GMR est le premier du genre axé sur les questions de renseignements financiers liées à un événement sportif majeur. Il combine les techniques traditionnelles de collecte de renseignements et l'expertise financière pour dévoiler des activités économiques illégales : fixation des prix, coûts excessifs, chantage, fraude contractuelle et vol de matériaux. La pénurie de main-d'oeuvre qui frappe l'industrie de la construction en C.-B. pousse aussi le groupe à faire enquête sur les liens possibles avec l'immigration illégale.

Le groupe a confié des enquêtes à des services de police municipaux ou partenaires fédéraux aux fins de suivi, mais les poursuites criminelles ne sont pas nécessairement le but ultime.

« Dans plusieurs cas, nous voulons atténuer le problème avant qu'il ne donne lieu à une poursuite », précise Graham.

Les stratégies d'atténuation comprennent informer les sociétés de construction et les gestionnaires de projet d'éventuels pièges et secteurs à améliorer, comme la qualité de la surveillance ou la sécurité sur place, et collaborer avec des partenaires pour inclure des dispositions sur l'accès à l'information dans d'importants marchés de construction.

« Que le marché nous permette d'avoir accès à de l'information qui nécessiterait normalement un mandat de perquisition », de dire Graham, qui ajoute que l'examen des dossiers financiers, de la structure de gestion d'une société et d'autres données importantes peut aider les enquêteurs à cerner les liens avec le crime organisé.

Les mesures visent à mettre fin à la fraude avant qu'elle ne commence, souligne Graham, et la plupart des entrepreneurs les approuvent. « La plupart des entrepreneurs et des sociétés qui participent à ces projets sont honnêtes et n'ont aucun lien avec le crime organisé... Ils ne veulent pas engager un sous-sous-entrepreneur qui leur causera des problèmes ».

Les activités du GMR s'ajoutent à d'autres mesures prises par des organismes partenaires chargés des travaux de construction en vue des Olympiques. Le COVAN, le ministère des Transports de la Colombie-Britannique, Canada Line Rapid Transit Inc., par exemple, utilisent des systèmes de gestion de qualité certifiés ISO 9000. Le COVAN demande aux entrepreneurs de tester régulièrement les matériaux de construction et de présenter les résultats pour les comparer aux données du comité issues de tests indépendants.

COVAN

Le tremplin de ski du centre Whistler, un projet d'aménagement en cours de construction pour les Jeux olympiques d'hiver de 2010 à Vancouver.

« Ainsi, nous nous assurons d'avoir un produit de qualité », affirme Dan Doyle, vice-président exécutif des travaux de construction du COVAN.

Doyle précise que les gestionnaires des travaux de construction du COVAN n'ont décelé « aucun signe d'activité frauduleuse » à ce jour, mais si c'était le cas, « nous n'hésiterions pas à faire appel au GIS de la GRC ».

Avec le développement de l'infrastructure bien engagé, la plupart des marchés de construction déjà attribués, le GMR commencera à surveiller le grand nombre de marchés de services d'alimentation, de transport, de loisirs et de nettoyage après les Jeux.

Les travaux à ce jour deviennent aussi un exemple à suivre pour les prochains Jeux olympiques, comme ceux de Londres 2012. « Ils nous demandent conseil, précise Graham, ils amélioreront ce que nous mettons en place. » ■

# Comment votre organisme détermine-t-il ses priorités en matière de fraude?

Les spécialistes

**Surint. Stephen Foster,** chef de la Sous-direction des infractions commerciales de la GRC
**Jonathan J. Rusch,** conseiller juridique spécial en prévention de la fraude, Division criminelle, Section de la lutte antifraude, département de la Justice des États-Unis
**Murray Taylor,** coordonnateur national - Opérations économiques et spéciales, Police fédérale australienne

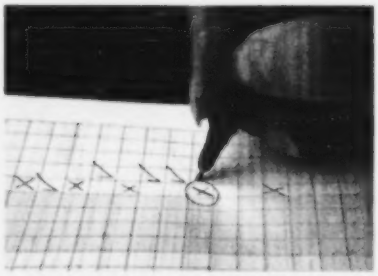
**Surint. Stephen Foster**

Le Programme des infractions commerciales de la GRC compte 27 groupes opérationnels établis dans plusieurs grandes villes au Canada. Il mise sur une stratégie multidimensionnelle pour la répression des diverses activités criminelles relevant de son mandat, dont les fraudes majeures, les fraudes en marketing de masse, la corruption et l'usurpation d'identité. Ce mandat comprend également la prévention du crime par l'éducation et la sensibilisation du public. Vu l'ampleur du contexte, je crois qu'il faut répondre à la question dans une optique générale.

Au plan organisationnel, la haute direction de la GRC fixe cinq priorités stratégiques nationales. L'intégrité économique en est une. Les quatre autres sont le crime organisé, la jeunesse, le terrorisme et les collectivités autochtones.

En évaluant les menaces, en dépouillant les reportages médiatiques et en examinant les demandes de service, les Infractions commerciales dégagent les nouvelles tendances les plus menaçantes en matière de fraude. C'est ainsi que nous en sommes venus à donner préséance à la répression de l'usurpation d'identité et de la fraude en marketing de masse. Le faux-monnayage, la fraude par carte de paiement et la corruption figurent aussi parmi nos priorités.

Les ressources étant limitées, nous devons trouver un équilibre entre les enquêtes sur les plaintes, les enquêtes axées sur le renseignement et les activités de prévention et de sensibilisation. C'est une question de jugement. Les gestionnaires des groupes opérationnels répartissent leurs ressources entre ces activités, compte tenu de préoccupations et de facteurs locaux.



Le Système de priorisation des dossiers opérationnels (SPDO) est un outil conçu par les Infractions commerciales pour aider les gestionnaires sur le terrain. Il s'agit d'un logiciel qui interprète 12 éléments relatifs aux enquêtes et attribue une cote numérique globale à chaque dossier. Une cote élevée exige une priorité élevée. Voici quelques-uns des critères évalués : le lien que présente l'infraction avec notre mandat; la somme d'argent en cause (plus elle est forte, plus la cote sera élevée); le temps écoulé depuis l'infraction (plus elle est récente, plus la cote sera élevée); la facilité de collecte des preuves (plus elle est grande, plus la cote sera élevée).

Au plan tactique, nos groupes opérationnels priorisent les enquêtes. Les gestionnaires tiennent compte de plusieurs facteurs, dont la cote du SPDO, les priorités stratégiques visées par l'enquête, le mandat des Infractions commerciales, les activités auxquelles la Sous-direction donne priorité, les ententes en vigueur (traités internationaux, protocoles d'entente, etc.), la somme d'argent en cause, les compétences spécialisées requises, les répercussions sur les victimes, la présence d'un lien avec la corruption, et enfin les facteurs locaux.

Le processus d'établissement des priorités en matière de fraude des Infractions commerciales de la GRC est bien équilibré. Il tient compte de nombreux facteurs, tant stratégiques que tactiques.

**Jonathan J. Rusch**

Le département américain de la Justice établit de trois façons ses priorités en matière de lutte antifraude. Premièrement, selon le plan stratégique 2007-2012 du Département, la Division criminelle a adopté un plan de gestion qui comprend les priorités suivantes :

- Assurer l'intégrité du gouvernement. Conformément à cette priorité, la Division criminelle vise la fraude électorale, la fraude en matière d'immigration et d'approvisionnement, la corruption publique liée à ces infractions et à d'autres infractions. Par exemple, le Département a créé des groupes de travail spéciaux sur la fraude en matière d'approvisionnement et les fraudes de tous genres qui ont fait suite aux ouragans Katrina, Rita et Wilma en 2005, et les fraudes liées à la reconstruction de l'Irak.
- Préserver et maintenir la confiance à l'égard des marchés. Conformément à cette priorité, la Division criminelle vise la fraude industrielle, la fraude par marketing de masse, le vol d'identité et la cybercriminalité.
- Décourager les crimes violents et le crime organisé. Conformément à cette priorité, la Division criminelle vise les crimes (y compris la fraude) commis par diverses organisations criminelles dans le but de faire des profits illicites ou de soutenir leurs opérations.
- Réprimer la criminalité transnationale.

Conformément à cette priorité, la Division criminelle vise les divers crimes transnationaux, comme le crime organisé et le cybercrime, fournit de la formation internationale et soutient activement l'établissement de liens en matière d'application de la loi.

Deuxièmement, de hauts représentants du Département et de la Division criminelle président des groupes de travail nationaux interorganismes axés sur certains genres de fraudes. Parmi ces groupes, on trouve le Bank Fraud Enforcement Working Group (fraude bancaire), le Corporate Fraud Task Force (fraude industrielle), le Mass-Marketing Fraud Working Group (fraude par marketing de masse), le Mortgage Fraud Working Group (fraude hypothécaire) et le Securities and Commodities Fraud Working Group (fraude en valeurs mobilières et sur les marchandises). De plus, le President's Identity Theft Task Force (vol d'identité) compte un sous-groupe responsable du droit criminel (Criminal Law Enforcement Subgroup). Chaque groupe se réunit régulièrement, ce qui permet aux représentants du Département et des organismes d'enquête fédéraux, comme le FBI, le Postal Inspection Service et le U.S. Secret Service, d'échanger de l'information sur certaines tendances en matière de fraude et de trouver des possibilités de collaboration entre les organismes pour faire enquête sur ces fraudes.

Troisièmement, le département de la Justice, sous la direction de la Division criminelle, a entrepris diverses initiatives proactives ayant pour cibles certaines fraudes. Il s'agit notamment de l'initiative Operation Roaming Charge (2004), qui ciblait tout particulièrement la fraude nationale et internationale par télémarketing, l'initiative Operation Global Con (2006), axée sur la fraude internationale par marketing de masse à laquelle se livraient des groupes criminels, et plusieurs opérations visant la délinquance économique en ligne. La portée de ces opérations est de plus en plus internationale du fait que les organismes d'application de la loi américains reconnaissent l'importance d'établir des relations de collaboration avec des organismes d'application de la loi du Canada et d'autres pays, et de collaborer aux enquêtes et aux poursuites transnationales.

**Murray Taylor**

La Police fédérale australienne (AFP) reconnaît que pour maintenir la confiance de la population, les pratiques commerciales pour contrer la fraude doivent être constamment améliorées et remaniées en fonction des nouvelles technologies et vulnérabilités.

Conformément au plan de lutte contre la fraude et la corruption établi par l'AFP pour l'exercice 2007-2009, diverses initiatives inspirées de meilleures pratiques en matière de lutte contre la fraude et la corruption ont été mises en oeuvre dans tous les secteurs fonctionnels de l'AFP.

Lors de l'élaboration du dernier plan de lutte contre la fraude et la corruption, l'AFP a mené des évaluations des risques dans l'ensemble de l'organisation en confiant le processus d'évaluation au groupe des entreprises. On a demandé à des gestionnaires et à des employés de décrire, d'analyser et d'évaluer les risques internes et externes et les menaces liées à leur propre secteur d'activités en fonction de catégories définies dans les Commonwealth Fraud Control Guidelines.

> **« Les organismes d'application de la loi américains reconnaissent l'importance d'établir des relations de collaboration avec des organismes d'application de la loi du Canada et d'autres pays. »**

Plusieurs risques ont été cernés et évalués dans l'ensemble de l'organisation. La catégorie la plus à risque était la gestion de la technologie de l'information et de la sécurité de l'information. Un autre secteur à risque était la gestion des relations avec les clients et les partenaires stratégiques afin d'appuyer leurs initiatives antifraude. Le commerce électronique, la prestation de services électroniques et l'Internet figuraient aussi parmi les secteurs jugés les plus prioritaires.

D'après les directives fournies par un comité de surveillance de haut niveau, toutes les questions de contrôle de la fraude et de la corruption sont examinées et classées par ordre de priorité selon la probabilité que les risques augmentent et apparaissent dans certaines unités fonctionnelles. L'efficacité des mesures prises à l'égard de tous les risques de fraude et de corruption est continuellement évaluée et les résultats sont communiqués au comité aux fins d'examen.

On donne à tous les risques résiduels intermédiaires au sein de certaines unités fonctionnelles une plus grande priorité aux fins de gestion et de contrôle. Les risques résiduels de niveau moindre, gérés à l'aide des contrôles internes existants, ne font pas l'objet d'autres mesures d'atténuation s'ils sont à un niveau acceptable.

Des analyses de l'environnement et un système d'analyse des plaintes en fonction de normes professionnelles assurent le contrôle du rendement et l'assurance de la qualité. L'accent est mis sur l'établissement des tendances de la corruption et de la fraude organisationnelle pouvant être contrées. À l'intérieur de ce modèle, les allégations de corruption font l'objet d'une surveillance indépendante par l'Australian Commission for Law Enforcement Integrity.

À l'externe, les statistiques sur la fraude de l'AFP sont transmises à l'Attorney-General's Department. De plus, selon les Commonwealth Fraud Control Guidelines, le commissaire confirme au ministre des Affaires intérieures, dans le rapport annuel de l'AFP, qu'il est convaincu que des procédures appropriées ont été adoptées en matière de prévention, de détection, d'enquête et de collecte de données sur la fraude.

Le plan actuel de lutte contre la fraude et la corruption permet d'intégrer l'évaluation des risques organisationnels et les processus d'établissement de rapports en reconnaissant que la détermination des risques fait partie intégrante de toutes les fonctions quotidiennes de l'AFP. ■

# Une atteinte personnelle

## La fraude d'identité contre le consommateur canadien

**Insp. Barry Baxter**
**Contrefaçon et Fraude d'identité**
**Sous-direction des infractions commerciales (GRC)**

La fraude d'identité – le vol et l'utilisation frauduleuse de données personnelles à des fins criminelles – est un des crimes qui connaît la plus forte croissance depuis le nouveau millénaire. En effet, on estime que l'utilisation frauduleuse de l'identité personnelle coûte aux consommateurs canadiens plus de 2 milliards $ par année.

Nos données personnelles et financières sont devenues un bien précieux. Elles peuvent être effectivement saisies par le biais d'escroqueries par Internet, par piratage informatique ou de bases de données et par des réseaux organisés de vol de courrier, puis vendues et achetées dans le cyberespace.

Étant donné les possibilités de profits élevés et le faible risque de détection, la fraude d'identité attise l'intérêt du crime organisé. Ces organisations s'unissent aux cybercriminels rusés qui, à l'origine, commettaient des attaques sensationnelles motivées par la notoriété, mais qui sont passés à des attaques furtives, ciblées et raffinées contre les bases de données personnelles du gouvernement et de sociétés privées.

L'acquisition et l'utilisation de données personnelles pour obtenir frauduleusement des documents d'identité authentiques ou pour créer des documents d'identité falsifiés posent également problème.

### Vol d'identité ou fraude d'identité?

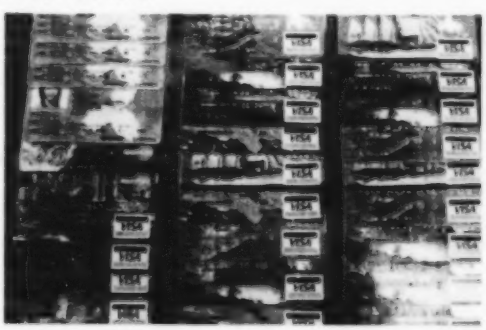
Le public et les médias continuent à parler de « vol d'identité » pour décrire cette activité criminelle. En réalité, votre identité est une entité qui ne peut pas vous être dérobée; on ne peut vous en priver. Par contre, on peut l'assumer pour une certaine période, mais vous conservez toujours votre identité. L'acte criminel en soi est à proprement parler la « fraude d'identité ».

L'utilisation frauduleuse d'une identité comprend deux actes distincts, relevant chacun d'un motif précis.

Le premier acte consiste à acquérir ou à voler des données personnelles ou financières. Il s'agit de stratagèmes ingénieux fondés sur Internet comme l'hameçonnage ou le détournement de domaine en vue d'inciter les citoyens à divulguer leur numéro de compte, leur mot de passe ou autres données personnelles. Il y a également des actes de piratage ciblant des bases de données d'envergure.

Les criminels se livrent en outre à l'examen de bases de données ouvertes à la recherche de données sur l'état civil en vue de créer des profils à partir de l'identité de personnes décédées. Une fois armés d'un nom et d'une date de naissance, les criminels sont à même de louer une boîte postale et un numéro de téléphone cellulaire grâce auxquels ils peuvent présenter une demande pour soi-disant faire remplacer un certificat de naissance, une carte de numéro d'assurance sociale (NAS), une carte-santé ou d'autres documents, ainsi que des cartes de crédit. À l'aide de ces documents, ils peuvent obtenir un passeport; ce faisant, ils auront constitué une identité fondée sur celle de personnes disparues.

Munis de quelques documents clés, les criminels peuvent demander et obtenir un passeport, et ainsi créer une identité complète à partir de celle d'une personne décédée.



Sous-direction des infractions commerciales

**Une fois armés d'un nombre suffisant de données personnelles et financières, les criminels peuvent prendre le contrôle de comptes bancaires, virer des fonds ou acquérir une marge de crédit.**

Au Canada, le gouvernement fédéral a récemment proposé une nouvelle législation dans le projet de loi C-27 selon lequel, s'il est adopté, commet une infraction quiconque, sans excuse légitime, fait fabriquer, a en sa possession, transmet, vend ou offre en vente une pièce d'identité concernant une autre personne, ou qui sciemment obtient, a en sa possession ou fait le trafic des données particulières d'une autre personne à des fins frauduleuses.

Pour le moment, le second acte – soit l'utilisation frauduleuse des données concernant une autre personne – constitue l'activité véritablement criminelle. Il peut s'agir de présenter une demande frauduleuse pour profiter de services ou de programmes gouvernementaux et pour obtenir des documents officiels délivrés par le gouvernement, ou pour acquérir des cartes de paiement. Une fois armés d'un nombre suffisant de données personnelles et financières, les criminels peuvent prendre le contrôle de comptes bancaires, virer des fonds ou acquérir une marge de crédit – le tout au nom d'une autre personne et ce, à son insu ou sans son consentement.

Par utilisation frauduleuse, on entend également la supposition de personne telle que définie à l'art. 403 du *Code criminel*, à savoir le fait d'assumer l'identité d'une personne, généralement en vue d'obtenir des biens ou des services comme la location d'un bureau ou d'un téléphone cellulaire. L'identité ainsi usurpée sert à masquer l'identité du coupable. Les identités systématiquement créées par des documents falsifiés ou obtenus frauduleusement favorisent également la capacité d'un criminel à voyager au pays et à l'étranger sous le couvert de l'anonymat.

### Cartes de paiement

La fraude par carte de crédit constitue dans les faits une fraude d'identité. Durant la courte période où on utilise une carte falsifiée pour une transaction, le criminel se prévaut frauduleusement de l'identité du détenteur légitime de la carte.

Sur le plan légal, une carte de paiement est soit une carte de crédit, soit une carte de débit. Les criminels peuvent obtenir les données magnétiques d'une carte sans l'autorisation du détenteur par une opération appelée écrémage. Le numéro d'identification personnelle (NIP) peut être saisi par une caméra cachée ou un faux clavier d'identification personnelle superposé au clavier légitime. Une fois armé des données magnétiques d'une carte et du NIP, un escroc peut fabriquer une carte falsifiée et l'exploiter pour obtenir des biens et des services.

Pratiquement toute fraude de carte de paiement relève du crime organisé. En 2006, les pertes totales causées par les fraudes combinées de cartes de paiement au pays a dépassé le million $ par jour. Ces recettes ont servi à financer des activités criminelles comme le trafic de drogues, l'achat d'armes, la contrebande, les prêts usuraires et la prostitution.

Une fois qu'on a déterminé l'occurrence d'une fraude, c'est l'institution financière émettrice du compte qui accuse la perte. De plus, l'institution impose un refus de service durant une courte période jusqu'au remplacement de la carte originale. Ces contraintes ont pour effet de miner la confiance des consommateurs à l'égard de la stabilité économique du Canada.

### De qui relève l'enquête sur les fraudes d'identité?

Tous les organismes d'application de la loi sont chargés d'enquêter sur les infractions prévues au *Code criminel*. La plupart des fraudes d'identité font intervenir une forme ou une autre de tromperie, de faux semblant ou de demande frauduleuse.

À la GRC, c'est le programme des infractions commerciales qui assume les enquêtes sur les fraudes d'identité qui ont une portée nationale ou internationale, par exemple lorsqu'un programme ou un service d'un gouvernement provincial ou du fédéral est visé ou lorsque l'intégrité de la base de données d'une institution a été compromise. Comme nombre de ces enquêtes sont de nature mondiale ou touchent l'Internet, les Infractions commerciales travaillent de concert avec la Sous-direction de la criminalité technologique pour le volet TI et avec le Bureau national de lutte contre la contrefaçon pour l'examen des documents en cause.

### Tendances en matière de fraude d'identité

Les organisations criminelles et les cybercriminels mettent à profit les avancées technologiques pour concevoir et exécuter des attaques réfléchies. Ils élaborent notamment des sites d'hameçonnage dans Internet destinés à reproduire des sites légitimes à partir desquels ils incitent des citoyens peu méfiants à fournir leurs données personnelles et financières qui seront par la suite utilisées frauduleusement.

La fréquence de ces attaques contre des bases de données du gouvernement et du secteur privé est une grande source de préoccupation. Ces actes de piratage visent notamment les organismes gouvernementaux, les bureaux de crédit, les fournisseurs de services, les institutions financières et d'autres détenteurs de vastes volumes de données. Selon les statistiques obtenues, les bases de données ainsi compromises relèvent à 40 pour cent d'entreprises privées, à 25 pour cent du gouvernement, à 20 pour cent du secteur de la santé et à 15 pour cent des institutions d'enseignement.

**Pratiquement toute fraude de carte de paiement relève du crime organisé. Ces recettes ont servi à financer des activités criminelles comme le trafic de drogues, l'achat d'armes, la contrebande, les prêts usuraires et la prostitution.**

De nombreux Canadiens exposent par ailleurs leurs données personnelles dans des réseaux sociaux comme Facebook et MySpace, ainsi que par l'intermédiaire de services de rencontre en ligne. Toutes ces entités sont vulnérables au piratage.

### Victimes

Au Canada, un grand nombre d'incidents de fraude d'identité ne sont pas signalés. Nombre des victimes hésitent à déclarer ceux-ci à la police par honte ou parce qu'elles estiment ne pas avoir de preuve à fournir aux autorités. Au sein de l'industrie des cartes de paiement, lorsqu'un site d'écrémage a été repéré, la société avise tous les détenteurs dont la carte a été compromise que celle-ci a été annulée et qu'ils en recevront une nouvelle. Mais comme le site en question n'est pas dévoilé, le détenteur ne peut pas signaler l'incident à la police.

Au pays, les détenteurs de données personnelles et financières ne sont pas tenus, que ce soit en vertu d'un règlement ou d'une responsabilité, de divulguer publiquement les violations de leurs mesures de sécurité – que ce soit aux victimes éventuelles ou aux organismes d'application de la loi. Ces dernières années, on a relevé un certain nombre de violations très médiatisées de bases de données qui ont fait un nombre étendu de victimes canadiennes.

La cote de crédit est un mécanisme qui permet aux citoyens d'obtenir du crédit, une hypothèque ou un prêt commercial. Lorsque la cote est compromise par une fraude d'identité, la victime doit fournir l'assurance au service de crédit qu'elle n'est pas responsable des factures impayées, du non-paiement d'un prêt et des modalités de recouvrement entamées contre elle. Cela peut prendre plusieurs années avant de rétablir son dossier de crédit. Le projet de loi proposé permettrait à un tribunal d'ordonner une réparation à l'endroit des victimes pour les dépenses engagées en vue de rétablir leur identité, de remplacer les documents d'identité et de rectifier leur dossier et leur cote de crédit. ■

---

Pour plus de renseignements sur la fraude d'identité et les recommandations en la matière, visiter le site ***www.rcmp-grc.gc.ca*** et cliquer sur les liens relatifs aux fraudes et escroqueries.

# Fraudes dans l'aide aux victimes

## Leçons tirées à la suite du passage de l'ouragan Katrina

**Par l'honorable David R. Dugas**
**Procureur de la Louisiane - district intermédiaire**
**Centre de commandement unifié du groupe de travail antifraude**

L'ouragan Katrina a frappé la côte du golfe du Mississippi tôt le matin, le lundi 29 août 2005. Les vents et l'onde de tempête ont détruit 69 000 résidences du Mississippi et ravagé toutes les collectivités côtières au sein de cet État.

La Louisiane n'a pas été balayée par les vents les plus dévastateurs, mais frappée par une importante onde de tempête. Érigée en grande partie sous le niveau de la mer, la Nouvelle-Orléans (Louisiane) est protégée par un système complexe de digues et de pompes. Peu après que les vents se sont calmés, on a appris que la digue de l'Industrial Canal avait cédé. D'autres bris de digues et une inondation générale dans toute la ville ont ensuite été signalés. À la tombée de la nuit, 80 % de la ville était inondée et plus de 200 000 maisons étaient détruites. Plus de 1,8 million de personnes ont fui la dévastation et déménagé partout aux États-Unis.

### Groupe de travail antifraude

Le ministère de la Justice des É.-U. a créé le groupe de travail chargé d'évaluer l'ampleur de la fraude liée à l'ouragan Katrina, le 8 septembre 2005, tout juste 10 jours après le passage de l'ouragan. Le ministère prévoyait que cette dévastation générale donnerait lieu à divers stratagèmes frauduleux dans diverses juridictions. Le groupe de travail devait créer une structure chargée de coordonner des milliers d'enquêtes de douzaines de forces policières fédérales et d'État et divers bureaux d'inspecteurs généraux dans de multiples juridictions.

Le groupe de travail est dirigé par Alice Fisher, procureure générale adjointe de la Division criminelle du ministère de la Justice, en collaboration avec les inspecteurs généraux et les directeurs des principales forces policières fédérales à Washington (DC). Le centre de commandement national de Baton Rouge (Louisiane) assure une coordination quotidienne et a dirigé la collecte, le contrôle, la rationalisation des enquêtes et la gestion des données. Les districts les plus touchés par les ouragans ont formé des groupes de travail dirigés par les bureaux des procureurs au sein de ces districts. Les districts sans groupe de travail ont désigné des personnes pour assurer la liaison entre le centre de commandement et le groupe de travail.

### La fraude après l'ouragan Katrina

Après Katrina, l'ampleur de la fraude allait de pair avec la portée des efforts de reprise des activités. Les habitants de la région touchée sont partis vers d'autres États à l'échelle du pays. Les opérations de recherche et sauvetage ont nécessité un soutien logistique sans précédent. On devait fournir à la région dévastée de la nourriture, de l'eau, de la glace, de l'essence, des génératrices, des outils de communication, des médicaments, des logements temporaires et des transports pour appuyer les secours. On a dû retirer plus de 100 millions de $vg^3$ de débris, rétablir les services, rouvrir les routes, réparer ou remplacer les installations gouvernementales avant de pouvoir amorcer les travaux de reconstruction.

La première leçon qui a été tirée après le passage de l'ouragan n'était pas nouvelle mais étroitement liée à l'ampleur de la fraude : la fraude suit l'attribution des fonds. La plupart des programmes de secours ont été la cible des fraudeurs dès que les régions touchées ont commencé à recevoir des fonds.

### Stratagèmes frauduleux

Les premiers stratagèmes frauduleux ont immédiatement suivi le désastre. De prétendues oeuvres de bienfaisance ont tenté de solliciter de l'argent à la population qui désirait faire des dons à tout organisme venant en aide aux sinistrés. En Floride, le site Web www.AirKatrina.com visait à obtenir des fonds soi-disant pour assurer les soins médicaux et les vols pour évacuer les habitants des régions touchées. À Bakersfield (Californie), des travailleurs

Huit jours après le passage de Katrina à la Nouvelle-Orléans, on ne percevait plus que le toit de ces maisons submergées. Les escrocs n'ont pas mis de temps pour exploiter des fonds de secours aux victimes et l'empathie du grand public.

David R. Dugas

engagés par la Croix-Rouge des É.-U. pour constituer un centre d'appels d'urgence ont commencé à soumettre des demandes pour eux-mêmes, leurs amis et associés. Plus de 80 de ces employés ont été accusés de fraude.

La Federal Emergency Management Agency (FEMA) a reçu plus de 2,5 millions de demandes de secours d'urgence provenant des personnes évacuées dans les 50 États, dont certaines étaient frauduleuses. En Oregon, en Floride, en Illinois, en Pennsylvanie, en Californie et dans plusieurs autres États, des personnes qui ne vivaient pas dans les régions dévastées et qui n'ont pas été touchées par les ouragans ont présenté de fausses demandes à la FEMA ou à la Croix-Rouge américaine, affirmant avoir été évacuées et avoir besoin de secours d'urgence. À ce jour, des poursuites ont été intentées contre ces fraudeurs par 41 des 93 bureaux des procureurs aux É.-U.

Souvent, les fraudeurs ont réussi à soutirer de l'argent parce que l'afflux de demandes empêchait les organismes de secours d'effectuer des vérifications. Lorsque les fraudeurs ont décelé cette faiblesse, ils ont élargi les stratagèmes. Certains ont présenté de multiples demandes, d'autres ont fait appel à des complices pour envoyer de fausses demandes en leur nom, en échange d'un montant d'argent. En Géorgie, une personne a envoyé au bureau du ministère du Travail de la Louisiane 51 demandes d'aide destinée aux chômeurs. En Floride, en Louisiane, au Mississippi, en Alabama, au Texas et même en Oregon, des poursuites ont été intentées contre des réseaux accusés d'exploiter systématiquement les programmes de secours d'urgence.

Parfois, la fraude était commise ou facilitée par des tiers. Dans un cas, un chef du service d'incendie et plusieurs collègues qui ont offert de travailler au centre médical de secours d'urgence de la FEMA à Baton Rouge ont été accusés d'avoir volé pour plus de 500 000 $ en fournitures médicales. Le chef du service d'incendie a aussi été accusé de tenter d'assassiner un membre de son équipe, croyant qu'il collaborait avec la police dans l'enquête menée sur le vol.

En Louisiane, des employés de la FEMA ont été poursuivis pour avoir proposé à des entrepreneurs de permettre une surfacturation dans leurs contrats en échange de pots-de-vin.

## Techniques d'enquête

Le défi d'enquêter sur la fraude après une catastrophe est souvent davantage de nature logistique que tactique. Il s'inscrit en général dans les modèles de comportement que la plupart des enquêteurs chevronnés connaissent bien, à savoir mentir, tricher et voler. Cependant, l'ampleur de la fraude peut sembler insurmontable pour les forces de l'ordre dans la région touchée et surprendre les services de police dans les régions éloignées de la zone sinistrée. Trouver, déployer et maximiser les ressources antifraude nécessaires peut être le plus grand et le principal défi des représentants des forces de l'ordre à la suite d'une catastrophe.

Pour enquêter sur des fraudes à la suite d'une catastrophe, les policiers doivent avoir des pistes d'enquête, accès à la preuve et aux ressources nécessaires pour faire leur travail et intenter les poursuites nécessaires. La meilleure façon d'obtenir des pistes et des éléments de preuve est de consulter la population et les données et dossiers internes des services de secours d'urgence.

Comme le nombre d'indices et de pistes peut mener au chevauchement et à la conduite d'enquêtes concurrentes par de multiples organismes, celles-ci doivent être coordonnées par un groupe de travail. Si la catastrophe est considérable, un centre de commandement spécial peut servir de point central de collecte, d'analyse et de communication des indices pour s'assurer d'éviter les chevauchements et les enquêtes concurrentes. Le groupe de travail et son centre de commandement peuvent aussi tenir lieu de répertoire central d'information pour déterminer où et comment obtenir les éléments de preuve pour faire enquête. Le groupe peut créer des protocoles pour simplifier la collecte et aider les enquêteurs à trouver des témoins et des documents.

Dans le cas du groupe de travail antifraude créé au lendemain de l'ouragan Katrina, la population a offert plusieurs des meilleurs indices à l'aide des numéros d'urgence fournis par le groupe de travail et menant au centre de commandement. Celui-ci reçoit et analyse les indices et plaintes provenant de diverses sources, vérifie l'information dans des bases de données, recueille les dossiers pertinents aux allégations de fraude et communique les indices et les informations au service de police compétent, qui s'occupera de faire enquête. Les indices et les informations sont versés dans la base de données du centre de commandement et vérifiés pour éviter les chevauchements. À ce jour, le centre de commandement a vérifié et transmis près de 14 000 indices qui ont permis d'intenter des poursuites contre plus de 830 fraudeurs.

Je recommande aux représentants des forces de l'ordre chargées d'enquêter sur ce genre de fraude de s'en tenir aux trois principes de base suivants :

1. Ne réinventez pas la roue. Vos policiers et enquêteurs savent comment s'acquitter de leurs tâches. Votre rôle consiste à vous assurer qu'ils ont les outils nécessaires pour faire leur travail. Tentez de répondre à leurs besoins dans le cadre des structures et des protocoles actuels.

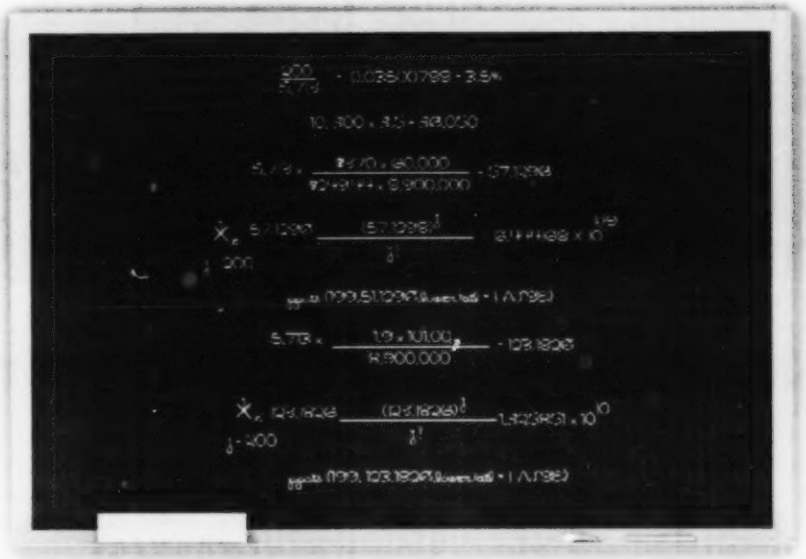
2. Ne créez pas de groupe de travail venant ajouter un autre niveau de supervision ou de commandement. Au sein du groupe de travail antifraude, le centre de commandement recueille, examine et analyse des pistes et les communique aux services d'enquête. Il ne gère pas les enquêtes ou ne demande pas aux agents de faire part du déroulement des enquêtes.

3. Misez sur la coopération, la communication et la coordination. Un groupe de travail peut accentuer l'efficacité en évitant les chevauchements ou les enquêtes concurrentes, en transmettant les indices selon l'expertise et les ressources d'un organisme, en facilitant les enquêtes de plusieurs corps de police et en fournissant des experts en la matière pour aider les policiers et les responsables des poursuites concernant les aspects particuliers de ce genre de fraudes. En misant sur la communication et la coopération, la force du groupe peut vite devenir impressionnante. Les divers organismes et le public en ressortent alors gagnants. ■

# FRAUDE DE LOTERIE

## Les mathématiques pour dénoncer des crimes

**Par le professeur Jeffrey S. Rosenthal**
**Département de statistique**
**Université de Toronto**



Dans la série télévisée Numb3RS, diffusée par CBS, l'enquêteur féru de mathématiques Charlie Eppes affirme avec audace que « tout est chiffres ».

Peut-être est-ce un peu exagéré, mais une enquête à laquelle j'ai récemment participé et qui portait sur une fraude de loterie m'a convaincu que l'analyse statistique pouvait se révéler un outil précieux pour détecter des actes frauduleux qui auraient pu sans cela rester cachés.

Nombreux sont les joueurs de loterie qui tendent simplement leur billet au vendeur du magasin du coin pour savoir s'ils ont gagné ou non. Un vendeur sans scrupule peut donc facilement prétendre que le client n'a rien gagné ou qu'il a gagné un prix insignifiant, pour réclamer plus tard lui-même le gros lot réellement remporté.

Mais telle malhonnêteté existe-t-elle vraiment?

En 2001, Bob Edmonds, un résident de 75 ans de Coboconk, en Ontario, a allégué qu'un détaillant local avait frauduleusement touché les 250 000 $ qu'il aurait dû gagner grâce à son billet de loterie. L'enquête qui s'ensuivit prouva qu'il avait raison et en 2005, au terme d'une longue bataille judiciaire (qui lui a coûté 425 000 $ en frais de justice), la Société des loteries et des jeux de l'Ontario (OLG) accepta de lui verser 150 000 $, sous réserve d'une ordonnance imposant le secret concernant l'arrangement. Cet élément éveilla des soupçons : la OLG dissimulait-elle d'autres histoires de gains de loterie frauduleusement encaissés par des employés de commerce? Pour l'émission The Fifth Estate du réseau anglais de Radio-Canada, je me suis penché sur les chiffres.

Exerçant son droit à l'information, Radio-Canada a pu établir qu'entre 1999 et 2006, 5 713 gros lots de loterie (de 50 000 $ et plus) ont été gagnés en Ontario, dont environ 200 (3,5 %) par des personnes qui travaillaient dans des magasins où l'on vend des billets de loterie. Cette dernière information tient compte uniquement des cas où le gagnant a reconnu qu'il travaillait dans un commerce, ce que certains gagnants ont pu délibérément cacher à la OLG. Ce nombre pourrait donc en réalité être supérieur à 200.

**Nombreux sont les joueurs de loterie qui tendent simplement leur billet au vendeur du magasin du coin pour savoir s'ils ont gagné ou non. Un vendeur sans scrupule peut donc facilement prétendre que le client n'a rien gagné, pour réclamer plus tard lui-même le gros lot.**

Combien de gros lots auraient dû être gagnés par ces vendeurs? Et quelle est la probabilité qu'ils aient pu en gagner 200, le plus honnêtement du monde, seulement grâce à leur chance?

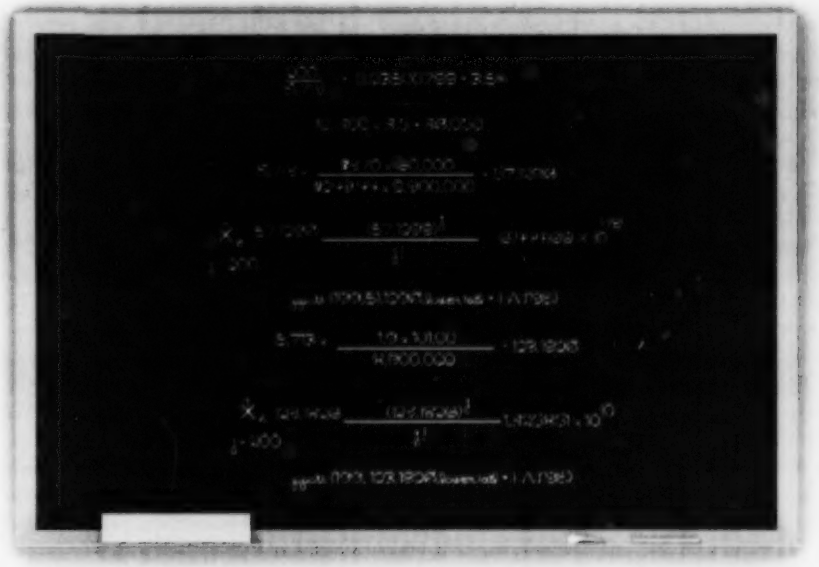
Pour répondre à ces questions, il fallait d'abord connaître le nombre de détaillants de billets de loterie. La OLG a répondu qu'elle ne connaissait pas la réponse, nous avons donc dû l'estimer à partir des chiffres dont nous disposions.

Il y a en Ontario 10 300 points de vente de billets de loterie. Une enquête de The Fifth Estate a indiqué qu'il y avait en moyenne 3,5 vendeurs par point de vente, donc 36 050 en tout. En revanche, un cadre de la OLG a déclaré en cour qu'il y avait 50 000 ou 60 000 vendeurs. Coup de théâtre, 5 jours avant la diffusion de l'émission (The Fifth Estate), la OLG présente de

# FRAUDE DE LOTERIE

## Les mathématiques pour dénoncer des crimes

**Par le professeur Jeffrey S. Rosenthal**
**Département de statistique**
**Université de Toronto**



Dans la série télévisée Numb3RS, diffusée par CBS, l'enquêteur féru de mathématiques Charlie Eppes affirme avec audace que « tout est chiffres ».

Peut-être est-ce un peu exagéré, mais une enquête à laquelle j'ai récemment participé et qui portait sur une fraude de loterie m'a convaincu que l'analyse statistique pouvait se révéler un outil précieux pour détecter des actes frauduleux qui auraient pu sans cela rester cachés.

Nombreux sont les joueurs de loterie qui tendent simplement leur billet au vendeur du magasin du coin pour savoir s'ils ont gagné ou non. Un vendeur sans scrupule peut donc facilement prétendre que le client n'a rien gagné ou qu'il a gagné un prix insignifiant, pour réclamer plus tard lui-même le gros lot réellement remporté.

Mais telle malhonnêteté existe-t-elle vraiment?

En 2001, Bob Edmonds, un résident de 75 ans de Coboconk, en Ontario, a allégué qu'un détaillant local avait frauduleusement touché les 250 000 $ qu'il aurait dû gagner grâce à son billet de loterie. L'enquête qui s'ensuivit prouva qu'il avait raison et en 2005, au terme d'une longue bataille judiciaire (qui lui a coûté 425 000 $ en frais de justice), la Société des loteries et des jeux de l'Ontario (OLG) accepta de lui verser 150 000 $, sous réserve d'une ordonnance imposant le secret concernant l'arrangement. Cet élément éveilla des soupçons : la OLG dissimulait-elle d'autres histoires de gains de loterie frauduleusement encaissés par des employés de commerce? Pour l'émission The Fifth Estate du réseau anglais de Radio-Canada, je me suis penché sur les chiffres.

Exerçant son droit à l'information, Radio-Canada a pu établir qu'entre 1999 et 2006, 5 713 gros lots de loterie (de 50 000 $ et plus) ont été gagnés en Ontario, dont environ 200 (3,5 %) par des personnes qui travaillaient dans des magasins où l'on vend des billets de loterie. Cette dernière information tient compte uniquement des cas où le gagnant a reconnu qu'il travaillait dans un commerce, ce que certains gagnants ont pu délibérément cacher à la OLG. Ce nombre pourrait donc en réalité être supérieur à 200.

**Nombreux sont les joueurs de loterie qui tendent simplement leur billet au vendeur du magasin du coin pour savoir s'ils ont gagné ou non. Un vendeur sans scrupule peut donc facilement prétendre que le client n'a rien gagné, pour réclamer plus tard lui-même le gros lot.**

Combien de gros lots auraient dû être gagnés par ces vendeurs? Et quelle est la probabilité qu'ils aient pu en gagner 200, le plus honnêtement du monde, seulement grâce à leur chance?

Pour répondre à ces questions, il fallait d'abord connaître le nombre de détaillants de billets de loterie. La OLG a répondu qu'elle ne connaissait pas la réponse, nous avons donc dû l'estimer à partir des chiffres dont nous disposions.

Il y a en Ontario 10 300 points de vente de billets de loterie. Une enquête de The Fifth Estate a indiqué qu'il y avait en moyenne 3,5 vendeurs par point de vente, donc 36 050 en tout. En revanche, un cadre de la OLG a déclaré en cour qu'il y avait 50 000 ou 60 000 vendeurs. Coup de théâtre, 5 jours avant la diffusion de l'émission (The Fifth Estate), la OLG présente de

nouveaux chiffres : il y aurait 140 000 vendeurs. En y regardant de plus près, on s'est aperçu qu'il s'agissait de 101 000 vendeurs actifs et de 39 000 ex-employés (roulement annuel) qui n'auraient pas dû rentrer dans les calculs.

Nous avions aussi besoin de savoir combien ces vendeurs dépensaient en billets de loterie comparativement à la population adulte en général. À nouveau, la OLG a répondu qu'elle l'ignorait. The Fifth Estate effectua donc une autre enquête qui permit d'arriver à la conclusion qu'en moyenne, une personne qui vendait des billets de loterie en achetait elle-même environ 1,5 fois plus que l'adulte moyen. La OLG tint sa propre enquête et arriva au résultat similaire de 1,9. La société Corporate Research Associates Inc. (CRA) mena une étude semblable dans les provinces du Canada Atlantique et obtint un résultat quasiment identique à celui de The Fifth Estate, soit 1,52.

Quelles conclusions tirer de tous ces nombres?

Si l'on part du principe que 60 000 vendeurs (le chiffre donné par la OLG en cour) ont acheté 1,5 fois plus de billets que l'adulte moyen (selon les enquêtes de The Fifth Estate et de CRA), on s'attendrait à ce que, en l'absence de fraude, les vendeurs aient gagné 57 des gros lots entre 1999 et 2006 – beaucoup moins que les 200 qu'ils ont effectivement empochés. La probabilité qu'ils aient remporté 200 gros lots ou plus par pure chance est infinitésimale, soit moins d'une chance sur un billion de billion de billion.

Même en prenant en considération les chiffres plus avantageux avancés par la OLG de 101 000 vendeurs dépensant en moyenne 1,9 fois plus en billets de loterie que la population adulte en général, on pourrait s'attendre à 123 gains importants par des vendeurs au cours de la période de référence. La probabilité qu'ils aient pu en remporter 200 ou plus resterait de toute façon en deçà d'une sur 7 milliards, ce qui est encore une fois, inimaginable.

Il est devenu évident que les vendeurs de billets de loterie gagnaient bien plus de gros lots qu'ils auraient dû par le simple jeu du hasard. Les statistiques avaient prouvé l'existence d'une fraude de loterie d'envergure.

Quant aux genres de commerces, on a constaté qu'un cinquième seulement des vendeurs de billets de loterie travaillaient dans des dépanneurs indépendants, mais que ces commerces étaient pourtant impliqués dans un pourcentage très élevé de cas de fraude. La OLG ne communiqua pas de chiffre exact à CBC, mais elle admit plus tard, dans la foire aux questions de son site web, que 53 % des vendeurs gagnants enregistrés travaillaient dans des dépanneurs. Ce nombre important ne peut être le fruit du hasard.

Il fut également très révélateur de considérer les propriétaires de commerces de détail comme un groupe distinct. Entre 1999 et 2006, ils avaient gagné environ 83 des gros lots. Nous ne connaissions pas le nombre exact des propriétaires de magasins (et la OLG ne voulait toujours pas nous aider), mais même d'après l'estimation la plus généreuse, il aurait dû y avoir tout au plus 25 propriétaires gagnants, certainement pas 83! La fraude devint encore plus évidente.

Après la diffusion de l'épisode de The Fifth Estate en octobre 2006, l'histoire a tout de suite fait les manchettes. La question a ouvert des débats à l'Assemblée législative ontarienne, le gouvernement a été mis sur la sellette et l'Ombudsman de l'Ontario a ouvert une enquête.

La OLG essaya d'abord de réfuter les conclusions statistiques, embaucha ses propres conseillers, nia l'existence d'une fraude de loterie importante et soutint que l'affaire Edmonds restait un cas isolé. Les preuves étaient toutefois accablantes. Lorsque l'Ombudsman rendit son rapport, cinq nouveaux cas de fraude avaient été dévoilés et la façon dont la OLG gérait la situation était sérieusement critiquée et jetait le discrédit sur l'organisme. Son président fut congédié et nombreux furent ceux qui pensèrent qu'il était grand temps d'apporter de profonds changements.

Le côté positif des choses est que la OLG a depuis mis en oeuvre des réformes stratégiques. Les consommateurs doivent maintenant signer leurs billets de loterie avant de les faire vérifier et des machines d'auto-vérification permettent aux clients de connaître leur lot avant même de remettre leur billet à qui que ce soit.

D'autres provinces se sont aussi penchées sur le problème. Peu après la mise en ondes de l'émission, l'Ombudsman de la Colombie-Britannique a ouvert une enquête similaire à l'issue de laquelle il a conclu que le système de loterie de Colombie-Britannique « rendait possible pour les commerçants d'empocher frauduleusement les gains des clients ». Le président de la British Columbia Lottery Corporation a lui aussi été renvoyé. Une autre étude que j'ai réalisée plus tard pour la Nova Scotia Gaming Corporation a révélé qu'entre 2001 et 2006, le nombre de gros lots gagnés par des commerçants de la province ne pouvait en aucun cas être attribué seulement à la chance, et que donc des vendeurs avaient là aussi fraudé des clients.

Des affaires comme celle-ci montrent à quel point les statistiques peuvent jouer un rôle important pour mesurer l'étendue d'un problème de fraude. Nous savons tous que des événements qui semblent a priori dus au hasard peuvent, s'ils se répètent, devenir une preuve tangible. Le défi est de reconnaître les situations où l'analyse statistique peut être utile, puis d'utiliser avec prudence la modélisation probabiliste pour déterminer si oui ou non les résultats observés peuvent être le fruit du hasard.

*Jeffrey S. Rosenthal est professeur au Département de statistique de l'Université de Toronto. Il est l'auteur de l'ouvrage* Struck by Lightning: The Curious World of Probabilities *(Harper Collins Canada, 2005).* ■

# Séduit par Internet

## Une opération policière conjuguée à la rescousse d'un Australien victime d'amaque

Un homme d'Australie méridionale victime d'une arnaque relative à un service de rencontre en ligne peut s'estimer chanceux d'être toujours en vie grâce aux réflexes de proches et l'intervention spontanée et la collaboration des services policiers.

Des Gregor, âgé de 56 ans, s'est rendu au Mali (en Afrique occidentale) le 26 juillet 2007 avec l'intention de rencontrer la femme qu'il pensait épouser. Au lieu, M. Gregor est devenu à son insu la cible d'une arnaque qui aurait pu avoir des conséquences tragiques.

Lorsqu'il est arrivé à Bamako (Mali), le 27 juillet, il a été accueilli comme prévu par deux Africains qui ont fait le nécessaire pour son arrivée. Après avoir recueilli ses bagages, M. Gregor a été amené à une autre personne qui l'a escorté jusqu'à une voiture.

Toutefois, plutôt que de l'emmener rencontrer sa future épouse, les trois hommes ont conduit M. Gregor à une demeure où on lui a enlevé ses vêtements, puis on l'a tenu en otage sous la menace d'une machette, avec la promesse d'une libération contre une rançon de 100 000 $. On lui a permis de contacter sa famille pour demander la somme exigée en prétextant des problèmes de carte de crédit.

Se doutant immédiatement de quelque chose et craignant pour la sécurité de M. Gregor, les proches de ce dernier ont alerté le ministère des Affaires étrangères et du Commerce australien. Des responsables de la police fédérale d'Australie (PFA), de la police d'Australie méridionale (PAM) et de l'ambassade canadienne au Mali ont alors pris contact avec la police nationale du Mali pour faire enquête et rapatrier M. Gregor en toute sécurité.

Le bureau de la PFA à Adélaïde a alors lancé l'opération Streambank, une opération policière conjuguée qui a mobilisé 50 agents de la PFA et 20 agents de la PAM. L'équipe, en service 24 heures sur 24, durant 12 jours, a intercepté des courriels et des appels téléphoniques adressés à la famille de la victime. Des membres du personnel aéronautique à l'aéroport d'Adélaïde et des enquêteurs de la PFA affectés à la police du territoire de la capitale ont également participé à l'enquête.

La PFA a détaché son agent de liaison principal d'Afrique du Sud au Mali, où ce dernier a travaillé de concert étroit avec l'ambassade canadienne et les autorités locales pour obtenir la libération de M. Gregor. Il s'agissait en outre de convaincre les kidnappeurs de permettre à la victime de se rendre à l'ambassade canadienne à Bamako pour y recueillir une rançon réduite (l'Australie ne compte pas de mission diplomatique au Mali).

Les ravisseurs sont tombés dans le panneau. Le 8 août, les ravisseurs de M. Gregor ont emmené celui-ci à l'ambassade, sous la menace que son amie et deux autres personnes – toutes des personnes fictives – seraient tuées s'il ne revenait pas aux ravisseurs. À l'ambassade, M. Gregor a été accueilli par l'agent de liaison de la PFA et des diplomates canadiens, qui lui ont dit de rester à l'ambassade, et qu'il était en sécurité. L'opération s'est déroulée sous la surveillance de plus de 25 policiers maliens de Bamako. Toutefois, les trois ravisseurs n'ont pas été appréhendés.

L'opération Streambank est un exemple éloquent de la coopération multiservices efficace entre la police d'État locale et nationale, et les autorités maliennes et canadiennes, grâce au réseau international de la PFA.

La PFA souhaite que cet exemple extrême serve d'avertissement aux citoyens et les incite à se prémunir contre des escroqueries de ce genre.

« Les criminels mettent Internet à profit pour leurrer un vaste auditoire, peu importe l'âge ou les antécédents de la victime; les gens doivent savoir qu'ils mettent leur vie en péril lorsqu'ils répondent à ces offres », explique Tim Morris, commissaire adjoint de la direction internationale de la PFA. « M. Gregor a été chanceux. Si ce fut une expérience éprouvante sur le coup, il s'en est tiré grâce à l'intervention de la PFA et à la collaboration multilatérale subséquente. »

L'agent fédéral Kevin Zuccato, directeur du Centre de la criminalité de haute technologie d'Australie, a participé à une émission radio nationale pour réitérer le message que les arnaqueurs vont continuer de cibler les gens et les inciter à envoyer de l'argent ou des présents, voire à voyager à l'étranger, sous de faux prétextes.

« Des gens comme Des Gregor sont séduits par Internet; les sites et les échanges de communication peuvent sembler tout à fait plausibles. Mais il faut exercer le même jugement qu'on manifesterait dans des situations réelles », prévient l'agent Zuccato. ■

D'après des dossiers de la revue Platypus et de la PFA

# L'écrémage

## Sensibilisation à la fraude en matière de cartes de crédit

**par le gend. Lloyd Schoepp**
**Section des infractions commerciales de la GRC à Calgary**

SIC de la GRC à Calgary

Au printemps 2006, la Section des infractions commerciales (SIC) de la GRC à Calgary et le Groupe de la criminalité économique du Service de police de Calgary (SPC) se sont réunis pour étudier une nouvelle pratique criminelle croissante, l'écrémage de cartes de crédit et de cartes de débit.

L'écrémage implique la copie non autorisée de données électroniques inscrites dans la bande magnétique des cartes de paiement. Les organisations criminelles sont à l'origine d'une grande part de cette pratique, qui croît à un rythme rapide à l'échelle nationale (en hausse de 34 pour cent en 2005-2006) et inflige à l'économie canadienne des pertes annuelles de millions de dollars.

L'écrémage ne se confine pas à une zone géographique précise du Canada; il faut donc adopter une démarche intégrée pour réprimer ce crime à l'échelle locale, nationale et internationale. Outre la nécessité d'une coopération, la SIC et le SPC ont proposé d'élaborer un programme de prévention.

Après avoir examiné divers programmes de prévention au pays, les enquêteurs du SPC et de la GRC se sont arrêtés sur le projet Protect. Ce programme de prévention et de sensibilisation au crime est issu d'un partenariat entre les organismes d'application de la loi, l'Association Interac, des sociétés de cartes de paiement et d'autres intervenants du secteur. Dans le cadre de ce programme, les agents de police se rendent dans les points de vente pour sensibiliser les gestionnaires et les employés sur la fraude en matière de carte de paiement. Le programme prévoit une formation pour les agents de première ligne et propose aux commerçants des conseils de prévention utiles.

Le programme a été lancé en novembre 2005 par le Service de police régional de Peel en collaboration avec huit services de police du sud de l'Ontario, l'Association Interac, des grandes sociétés de cartes de crédit et des détaillants d'essence. Le programme s'inspirait d'une initiative similaire mise en oeuvre au Québec en 2002 par le Service de police de Longueuil. Ce projet initial, axé sur les stations d'essence, s'est soldé par une diminution sensible de l'écrémage – jusqu'à 60 pour cent dans ces établissements.

En 2006, le SPC et la GRC en Alberta ont collaboré avec l'Association Interac au lancement du programme dans la région métropolitaine de Calgary et dans le sud de la province.

À cet égard, les membres du SPC et de la GRC ont suivi des séances de formation à Calgary et à Lethbridge sur l'écrémage et les modalités du projet. À Calgary, le projet a d'abord été mis à l'essai dans le district du SCP et dans six détachements ruraux et urbains de la GRC.

Les services de police ont obtenu des exemplaires de brochures utilisées par l'Association Interac en Ontario qu'ils ont adaptées pour les besoins du SPC et de la GRC.

À l'été 2007, on a fait le bilan du projet pilote pour en déterminer l'efficacité en vue de l'élargir à toute l'Alberta. La réaction des commerçants au projet a été extrêmement positive; ces derniers ont loué les efforts des policiers qui se sont rendus dans leur établissement pour les sensibiliser à l'écrémage des cartes de paiement. Le projet s'est également avéré utile lorsqu'un commerçant, après avoir appliqué les recommandations décrites dans le projet, a découvert un clavier d'identification personnelle trafiqué, puis a alerté la police.

En septembre 2007, on a tenu des réunions avec l'Association Interac pour déterminer l'orientation future du programme; on a alors établi d'autres endroits où mettre en oeuvre le programme.

De plus, les membres du SPC et de la GRC ont rencontré une institution financière albertaine pour lancer un projet pilote qui verrait à la distribution à de nouveaux points de vente des brochures du projet Protect affichant une raison sociale. On élargira ainsi la portée du programme de prévention.

Si des défis demeurent – notamment celui de susciter l'adhésion des membres dans les détachements occupés et de trouver d'autres modes de prestation du programme lorsque les ressources sont limitées –, les membres de la GRC et du SPC vont poursuivre leur collaboration avec les partenaires des milieux de la police et du commerce pour étendre le programme dans l'Alberta et favoriser la sensibilisation aux mesures de prévention de l'écrémage. ■

---

Pour plus de renseignements sur le projet Protect, communiquer avec l'Association Interac à **www.interac.ca**

# Escroqueries nigérianes sur les droits payables d'avance

**par Olaolu Adegbite**
**Section de la lutte aux escroqueries sur les droits payables d'avance**
**Commission nigériane contre les délits économiques et financiers**

Les arnaqueurs nigérians ont stupéfait le monde à la fin des années 80 par l'ingéniosité, la complexité et l'ampleur de leurs escroqueries sur les droits payables d'avance (DPA). Ce n'est qu'en 1991 qu'on a pu brosser un portrait précis du modus operandi qui valait à ces fraudeurs rusés des recettes annuelles de multiples millions de dollars. Leur nombre au pays et celui de leur cible à l'étranger se sont décuplés. Les escrocs ciblaient leurs victimes par courrier ordinaire, par télécopieur et par téléphone aux quatre coins du monde.

En 2000, le problème avait atteint une ampleur phénoménale, grâce essentiellement au recours efficace à la technologie de l'information. Ces criminels en col blanc sans vergogne ont redoublé d'audace devant l'inefficacité des autorités nigérianes. Ils vivaient dans l'opulence et se faisaient passer pour des philanthropes. À l'instar des barons de la drogue en Amérique du Sud et des mafiosi d'Italie dans les années 70, ils sont aussi devenus politiciens.

Le peuple nigérian a payé un lourd tribut. Tous les citoyens se sont vu accoler l'image d'escrocs par les intérêts étrangers. Les entreprises internationales ont été effrayées par la réputation douteuse du Nigeria, et les investissements étrangers directs ont chuté. À la fin de 2002, le Groupe d'action financière international (GAFI) contre le blanchiment d'argent a placé le Nigeria sur sa liste des pays non coopératifs. Et Transparency International a coté le pays parmi les nations les plus corrompues à son Index des perceptions de la corruption.

## Une lutte acharnée

La mise sur pied en avril 2003 de la Commission nigériane contre les délits économiques et financiers (Economic and Financial Crimes Commission, dite EFCC) a modifié la donne. Des mesures de répression rigoureuses, par voie d'arrestations, de poursuites, de renseignements, de prévention, de sensibilisation publique, de perturbation et de saisie de biens se sont soldées par une réduction sensible des escroqueries sur les DPA et autres délits économiques et financiers au Nigeria. Les bénéfices ont été immédiats et tangibles : croissance économique intense, amélioration de la réputation nationale et de la gouvernance politique, et rétablissement de la confiance chez les investisseurs étrangers.

La police a mis la main sur ce matériel rudimentaire servant à contrefaire des documents d'identité au Nigeria.

EFCC

L'EFCC a réduit l'attrait du pays pour les fraudeurs. Nombre d'entre eux ont renoncé à leur vocation illicite, tandis que quelques professionnels n'ont fait qu'émigrer dans des milieux moins hostiles où ils ont pu continuer à perpétrer leurs crimes de cupidité avec moins de risques matériels. De fait, la sous-région de l'Afrique de l'Ouest, plus particulièrement le Ghana, le Togo, la République du Bénin, le Burkina Faso, le Mali et la Côte d'Ivoire, a connu une hausse marquée d'activités liées aux fraudes sur les DPA depuis 2004. Le même constat s'applique à l'Afrique du Sud, au Royaume-Uni, à la Hollande, à l'Espagne, aux Émirats arabes unis et au Canada. Il est futile de prétendre que des Nigérians ne sont pas impliqués dans ces chaufferies établies à l'étranger.

Contrairement à ce que certains théoriciens ont suggéré, nous n'avons pas encore établi de liens concrets entre les réseaux nigérians d'escroqueries sur les DPA et d'autres organisations criminelles internationales, dont celles d'Europe de l'Est, les grands réseaux de trafiquants de stupéfiants, de traite des personnes ou de cellules terroristes.

L'EFCC a déposé plus de 300 accusations dans des affaires d'escroqueries sur les DPA devant plusieurs hauts tribunaux nigérians; toutefois, aucune de ces affaires ne concernait d'actes de violence. En outre, aucun de ces fraudeurs n'a manifesté la volonté délibérée de s'allier à une organisation criminelle étrangère précise. Leurs activités se font de manière fluide, anonyme et au fi des frontières. Dans certains cas, les escrocs nigérians ont obtenu des données de cartes de crédit depuis des sites de pirates vietnamiens ainsi que d'autres sites en Roumanie, en Russie et aux États-Unis.

À la lumière des renseignements dont on dispose et des tendances et de l'expérience récentes, on peut hasarder quelques hypothèses sur l'évolution future des escroqueries sur les DPA :

- Le nombre de fraudeurs sur les DPA diminuera. Toutefois, ceux qui

survivront seront plus puissants et efficaces.

- Les stratégies de promotion actuelles, qui font surtout appel à la cupidité de la victime (stratagèmes axés sur des contrats, des virements de fonds, de l'argent noir, des successions, des loteries, des pierres précieuses et du pétrole brut), cibleront désormais les émotions (stratagèmes visant des animaux domestiques, des oeuvres de bienfaisance, la religion et les relations romantiques).
- Les bases opérationnelles passeront en Europe et en Amérique du Nord afin de susciter un faux sentiment de sécurité chez les victimes potentielles (le Nigeria ne figurera à aucun stade de l'escroquerie). En outre, les autorités judiciaires de ces pays axent la répression principalement sur les crimes violents.
- On constatera une participation croissante de ressortissants d'autres pays dans les escroqueries sur les DPA, surtout de pays où sont présentement établies les chaufferies.
- Les escrocs tireront de plus en plus parti des lacunes actuelles sur le plan de la collaboration policière internationale, des lacunes législatives de certains territoires, des congestionnements bureaucratiques dans le traitement des demandes en vertu de traités d'entraide juridique, des lacunes de renseignements, des procédures fastidieuses d'extradition, du manque d'échange de renseignements au sein de la communauté policière, des lois strictes sur la divulgation et des exigences fondamentales.
- On verra un recours accru aux microstations (VSAT), au mode voix sur IP et aux serveurs mandatés de la part des escrocs pour se soustraire à toute détection.
- On verra un nombre accru de victimes réparties dans des zones étendues avec l'accessibilité grandissante d'Internet large bande, mais les pertes combinées pour ces nouveaux utilisateurs seront beaucoup plus faibles comparées à celles des victimes en Amérique du Nord et en Europe. Les régionsc d'Asie, du Moyen-Orient et de l'Australie connaîtront davantage de victimes que l'Amérique du Nord, compte tenu des mesures de prévention mises de l'avant aux États-Unis et au Canada.
- Les escrocs élargiront leurs connaissances et développeront leurs capacités technologiques pour se livrer à des intrusions afin d'obtenir par eux-mêmes les données de compte, plutôt que de s'en remettre à des pirates informatiques.
- Les attaques par mystification et hameçonnage s'intensifieront avec l'introduction récente des systèmes de paiement électronique au Nigeria et avec l'expérience grandissante des escrocs.
- Les réseaux de paiement électronique remplaceront Western Union et MoneyGram comme principal moyen de recevoir les profits des fraudes sur les DPA.
- Le recours aux services de poste et de messagerie s'intensifiera considérablement dans les pays voisins du Nigeria, surtout en République du Bénin, au Ghana et au Togo, pour l'exportation de faux instruments financiers et la réception des trousses de fraude dans Internet.
- La contrefaçon à grande échelle de chèques bancaires, de mandats, de certificats-cadeaux, de chèques de voyage et d'autres instruments financiers utilisés dans les fraudes sur les DPA ira grandissant en Amérique du Nord et en Europe.
- Les crimes sur les DPA seront toujours motivés par l'argent, et les criminels vont continuer d'éviter les crimes violents.

Les fraudeurs sur les DPA sont des adversaires rusés et pleins de ressources qui auront peu de difficulté à évoluer et à élaborer des contre-mesures pour déjouer les initiatives de répression. Cela dit, nous estimons qu'une synergie dynamique entre les organismes d'application de la loi et l'industrie – en particulier les fournisseurs de services postaux, bancaires, de messagerie, de virement de fonds, de télécommunications et d'Internet – est essentielle à l'élaboration et à la mise en oeuvre de mesures stratégiques pour réprimer les fraudes sur les DPA, car mieux vaut prévenir que guérir. ■

### Fraude en matière de frais payables à l'avance : la lutte menée par le Canada

Au cours des dix dernières années, certaines villes de l'Ontario, du Québec, de la Colombie-Britannique et de l'Alberta sont devenues les bases des activités frauduleuses d'Afrique occidentale au Canada. Voici comment les organismes d'application de la loi canadiens combattent ce fléau :

- Répression : Six partenaires régionaux, incluant trois groupes d'intervention, font enquête sur les organisations de fraude par marketing de masse, dans certaines villes comme Montréal, Toronto et Vancouver, afin de les perturber et de les démanteler.
- Saisie : Programme permettant de saisir l'argent et les titres négociables associés à la fraude au Canada. Par exemple, le programme de la Colombie-Britannique a permis de saisir en 2005 de l'argent et des titres négociables d'une valeur approximative de un million de dollars ainsi que des faux chèques (d'une valeur de 118 M$), dont plusieurs auraient été utilisés par les victimes.
- Perturbation : À Montréal, un programme recueille des renseignements de police afin d'identifier les entreprises de vente sous pression, puis dépêche des policiers sur les lieux afin d'interroger les employés. Souvent, les fraudeurs cessent, déménagent ou reportent leurs opérations simplement parce qu'ils se sentent visés par la police. Dans d'autres cas, la police exécute des perquisitions ou procède à des arrestations.
- Renseignements : Un projet présentement en cours vise à fusionner deux bases de données sur les plaintes de fraude au Canada (bases de données du Centre d'appel antifraude du Canada et du Centre de signalement en direct des crimes économiques) en un seul répertoire pour l'échange de renseignements et d'information.

# L'industrie du vin et la lutte contre la contrefaçon

## Les techniques de l'industrie donnent aux consommateurs des moyens d'agir

*Les produits contrefaits ont pour effet non seulement d'enrichir les organisations criminelles mais également de miner la crédibilité des fabricants de bonne foi, car les consommateurs croient qu'ils ont été dupés. Depuis longtemps victimes de la contrefaçon, les fabricants de vin ripostent maintenant grâce à un nouveau processus d'authentification de pointe créé par la société suisse Algoril. Olivier Gudet, directeur des ventes d'Algoril, explique comment le processus cible les faussaires à la base.*

**Par Olivier Gudet**
**Directeur des ventes, Algoril**

La mondialisation des échanges commerciaux a de quoi réjouir les faussaires. À mesure que les fabricants étendent leurs marchés géographiques, plusieurs produits se retrouvent entre les mains de groupes « spécialisés » dans la création de contrefaçons. Les fabricants doivent donc trouver des moyens simples et efficaces de décourager les faussaires et de détecter tôt les contrefaçons.

Dans l'industrie du vin, notamment, plusieurs solutions reposent sur des techniques invisibles, p. ex. utiliser des encres ou des papiers spéciaux, à l'instar des billets de banque. Devenues désuètes, ces techniques coûtent cher et sont difficiles à utiliser car elles nécessitent des scanneurs ou des détecteurs spéciaux. Ces solutions cachées ne rassurent pas les consommateurs qui, souvent, ignorent même leur existence.

La solution qu'offre la société Algoril à l'industrie du vin pour lutter contre la contrefaçon est simple et efficace : un code unique est attribué à chaque bouteille de vin produite, qui devient essentiellement l'empreinte digitale du produit.

### Protéger les produits authentiques

Chaque code d'identification Algoril est créé en combinant l'information sur les caractéristiques d'un vin (producteur, appellation, millésime et numéro de série) à un algorithme de chiffrement. En général, le code est imprimé de façon manuelle sur la contre-étiquette de la bouteille et l'information sur le produit est conservée dans une base de données à haute sécurité de la société Algoril. Il est possible d'inscrire un deuxième code sur une matrice qui peut être lu à l'aide d'un scanneur ou d'une caméra de téléphone cellulaire.

Les consommateurs peuvent ensuite vérifier l'authenticité d'un produit en envoyant une demande par le biais du site Web de la société Algoril ou d'un service de messagerie textuelle. L'information dans la base de données d'Algoril est comparée à celle qui est inscrite sur le produit, telle qu'elle a été envoyée par le consommateur. Cette contre-vérification permet de détecter plusieurs types de fraude, comme les marchés parallèles ou la contrefaçon.

Pour les producteurs, la technique de codage ne nuit pas à leurs activités car les étiquettes codées sont livrées prêtes à être utilisées. Le coût est minime en raison des dispositifs d'impression pouvant produire différents types d'étiquettes sans nuire à la qualité ou au résultat d'impression.

De plus, les consommateurs peuvent en tout temps avoir accès à l'information sur les produits, ce qui est très avantageux, tandis que les mesures anticontrefaçon actuelles exigent d'attendre que le producteur ou un dispositif spécialisé confirme qu'il y a fraude.

### Détecter les contrefaçons

Vous saurez que votre bouteille est une contrefaçon si après avoir envoyé une demande de vérification à la société Algoril, vous apprenez que le code n'est pas ou ne correspond pas à l'information enregistrée dans sa base de données.

Un autre signe qui ne ment pas : si plusieurs demandes de vérification portent sur la même bouteille; en général, ceci signifie qu'un faussaire a « cloné » un ou plusieurs codes. Dans ces cas, les données de traçabilité fournies par le fabricant pour chaque lot de bouteilles commercialisé peuvent permettre de savoir exactement ou la bouteille originale a été achetée. Ces données comprennent l'information sur la production du vin et des détails sur l'expédition, comme le pays de destination, l'importateur, l'exportateur et le détaillant.

En vérifiant les données de traçabilité en fonction de l'information contenue dans la demande de vérification originale, on peut aussi détecter des marchés parallèles

et déterminer si un lot donné a été détourné de sa destination originale. Si l'information diffère, le système produit une alarme de détection de fraude et envoie un courriel au producteur. Celui-ci doit alors contrôler chaque maillon dans la chaîne de distribution pour déterminer qui a détourné le lot.

## Participation des consommateurs

Le succès des techniques d'Algoril dépendra de la mesure où les consommateurs sont incités à utiliser les codes pour obtenir de l'information. Au départ, un consommateur dans un point de vente au détail de vin peut s'assurer de l'authenticité d'une bouteille avant de l'acheter. Vérifier un code permet aussi aux consommateurs d'obtenir d'autres renseignements utiles sur la bouteille de vin, p. ex. température idéale de service, mets à consommer avec ce type de vin.

Ces demandes du consommateur donnent en quelque sorte des « pistes » au système. Pas besoin d'outils de détection spécialisés et coûteux, car la fraude est détectée directement ou indirectement par le biais des actions des consommateurs.

L'étendue de l'information fournie dépend de l'auteur de la demande, étant donné que les acheteurs finals et les responsables de l'industrie n'ont pas besoin des mêmes détails. Par exemple, le consommateur a besoin de connaître la « valeur » du produit, tandis que les autorités sanitaires s'intéresseront plutôt à la composition du vin et aux dates de consommation. Chaque requérant, s'il est identifié, recevra l'information formatée en fonction de ses besoins.

## Perspectives d'avenir

La grande attention que portent les médias aux opérations de contrefaçon est attribuable aux lots contrefaits de vins réputés vendus aux enchères. Malheureusement, il n'y a rien à faire lorsque les bouteilles sont déjà en circulation et n'ont pas de code d'identification. Pour vérifier l'authenticité de ces vins, on doit ouvrir les bouteilles, goûter ou tester le vin, ce qui cause des problèmes, car ceci a pour effet d'altérer le vin de façon permanente. Même en testant juste une bouteille dans un lot, rien ne garantit que les autres bouteilles soient authentiques.

Les scellés qu'on peut mettre sur le goulot des bouteilles pour éviter qu'elles ne soient altérées ne sont pas une solution idéale non plus. Des faussaires ont déjà fait un trou sous une bouteille, qu'ils ont vidée et remplie d'un autre vin en bouchant le trou avec de la colle acrylique. À l'oeil nu, rien n'indiquait que la bouteille avait été altérée. Même si elle avait été scellée, le sceau serait resté intact.

Aujourd'hui, le seul moyen de dissuasion efficace est d'assurer un contrôle strict de la traçabilité, et ce, du début à la fin. Lorsqu'une fraude est détectée, nous faisons enquête pour déterminer à quelle étape précise de la chaîne logistique l'activité illicite a eu lieu.

Les producteurs doivent agir à la source. Les consommateurs doivent ensuite être encouragés à tirer profit des mesures qui leur sont offertes pour mettre fin à la contrefaçon. ■

*Suite de la page 2*


Waite, Mélanie. *Protection des renseignements personnels et protection contre l'escroquerie : guide pratique canadien*, Ottawa (Ont., Canada), Gendarmerie royale du Canada, HV 6685 .C2 W13f 2007

Wells, Joseph T. *Principles of Fraud Examination*, Hoboken (NJ, É.-U.), John Wiley, HV 8079 .F7 W46 2005

Williams, Alan Lee. *Occupational Fraud and Abuse Within Canada's Department of national Defense*, Utica (NY, É.-U.), inconnu, HV 6699 .C2 W67 2006

**Articles**

Brody, Richard G. « *Natural Catastrophe and Disaster Fraud: Calamity Criminals* », Fraud Magazine, vol. 20, no 6 (2006), pp. 28-31, 51.

Carozza, Dick. « *Fighting Fraud With Research* », *Fraud Magazine*, vol. 20, no 5 (2006), pp. 32-36.

Gober, Thomas D. « *Insidious Side Letters: Shady Business on the Side* », Fraud Magazine, vol. 20, no 4 (2006), pp. 25-27, 50.

Hoitfretter, Robert E. « *Latest Debit Card Fraud Schemes: Part 1 - Security Breaches Allow Data Thefts* », Fraud Magazine, vol. 20, no 4 (2006), pp. 32-35, 52-53.

Hoitfretter, Robert E. « *Latest Debit Card Fraud Schemes: Part 2 - Industry Initiatives, Technology and Global Legislation* », Fraud Magazine, vol. 20, no 5 (2006), pp. 42-43, 50-53.

Lautischer, Pierre E. « *Pension Fraud: Nabbing Bosses Who Crack Nest Eggs* », Fraud Magazine, vol. 21, no 1 (2007), pp. 32-35, 50-51.

Liberti, Francesco. « *Environmental Fraud: More Subtle Than Midnight Dumping* », Fraud Magazine, vol. 20, no 6 (2006), pp. 32-34, 47, 50.

Lion, Courtney J. « *What Asset Forfeiture Teaches Us About Providing Restitution in Fraud Cases* », Journal of Money Laundering, vol. 10, no 3 (2007), pp. 215-276.

Luby, Dwayne. « *Pharmacy Fraud: A Clear Prescription Part 1* », Fraud Magazine, vol. 21, no 3 (2007), pp. 24-27, 47.

Luby, Dwayne. « *Pharmacy Fraud: A Clear Prescription Part 2* », Fraud Magazine, vol. 21, no 4 (2007), pp. 20-23, 43-45.

McFadden, Michael. « *Fraud Investigations: A Case Study in Economic Evaluation* », Policing: An International Journal of Police Strategies and Management, vol. 25, no 4 (2002), pp. 752-761.

Poulos, Andrew. « *Illegal I.D.'s* », Law Enforcement Magazine, vol. 31, no 4 (2007), pp. 104, 106-111.

Svenson, Torleif. « *Global Fraud: Investigating Suspected Fraud in the Middle East* », Fraud Magazine, vol. 20, no 5 (2006), pp. 24-27.

Wangon, Sierra D. « *Fraud and the Factor of Fear* », *Fraud Magazine*, vol. 20, no 5 (2006), pp. 28-31, 47, 58.

**Sites Web**

Association of Certified Fraud Examiners
http://www.acfe.com

Fraud and Scam Reference
http://www.scambusters.com/scambusterscommonfraud.html

Investigator.com
http://www.investigator.com/links/insurancefraud.html

National Fraud Information Center
http://www.fraud.org

et déterminer si un lot donné a été détourné de sa destination originale. Si l'information diffère, le système produit une alarme de détection de fraude et envoie un courriel au producteur. Celui-ci doit alors contrôler chaque maillon dans la chaîne de distribution pour déterminer qui a détourné le lot.

### Participation des consommateurs

Le succès des techniques d'Algoril dépendra de la mesure où les consommateurs sont incités à utiliser les codes pour obtenir de l'information. Au départ, un consommateur dans un point de vente au détail de vin peut s'assurer de l'authenticité d'une bouteille avant de l'acheter. Vérifier un code permet aussi aux consommateurs d'obtenir d'autres renseignements utiles sur la bouteille de vin, p. ex. température idéale de service, mets à consommer avec ce type de vin.

Ces demandes du consommateur donnent en quelque sorte des « pistes » au système. Pas besoin d'outils de détection spécialisés et coûteux, car la fraude est détectée directement ou indirectement par le biais des actions des consommateurs.

L'étendue de l'information fournie dépend de l'auteur de la demande, étant donné que les acheteurs finals et les responsables de l'industrie n'ont pas besoin des mêmes détails. Par exemple, le consommateur a besoin de connaître la « valeur » du produit, tandis que les autorités sanitaires s'intéresseront plutôt à la composition du vin et aux dates de consommation. Chaque requérant, s'il est identifié, recevra l'information formatée en fonction de ses besoins.

### Perspectives d'avenir

La grande attention que portent les médias aux opérations de contrefaçon est attribuable aux lots contrefaits de vins réputés vendus aux enchères. Malheureusement, il n'y a rien à faire lorsque les bouteilles sont déjà en circulation et n'ont pas de code d'identification. Pour vérifier l'authenticité de ces vins, on doit ouvrir les bouteilles, goûter ou tester le vin, ce qui cause des problèmes, car ceci a pour effet d'altérer le vin de façon permanente. Même en testant juste une bouteille dans un lot, rien ne garantit que les autres bouteilles soient authentiques.

Les scellés qu'on peut mettre sur le goulot des bouteilles pour éviter qu'elles ne soient altérées ne sont pas une solution idéale non plus. Des faussaires ont déjà fait un trou sous une bouteille, qu'ils ont vidée et remplie d'un autre vin en bouchant le trou avec de la colle acrylique. À l'oeil nu, rien n'indiquait que la bouteille avait été altérée. Même si elle avait été scellée, le sceau serait resté intact.

Aujourd'hui, le seul moyen de dissuasion efficace est d'assurer un contrôle strict de la traçabilité, et ce, du début à la fin. Lorsqu'une fraude est détectée, nous faisons enquête pour déterminer à quelle étape précise de la chaîne logistique l'activité illicite a eu lieu.

Les producteurs doivent agir à la source. Les consommateurs doivent ensuite être encouragés à tirer profit des mesures qui leur sont offertes pour mettre fin à la contrefaçon. ■

...Suite de la page 2


Waite, Mélanie. *Protection des renseignements personnels et protection contre l'escroquerie : guide pratique canadien*, Ottawa (Ont., Canada), Gendarmerie royale du Canada. HV 6685 .C2 W13r 2007

Wells, Joseph T. *Principles of Fraud Examination*, Hoboken (NJ, É.-U.), John Wiley. HV 8079 .F7 W46 2005

Williams, Alan Lee. *Occupational Fraud and Abuse Within Canada's Department of national Defense*, Utica (NY, É.-U.), inconnu. HV 6699 .C2 W67 2006

**Articles**

Brody, Richard G. « *Natural Catastrophe and Disaster Fraud: Calamity Criminals* », Fraud Magazine, vol. 20, no 6 (2006), pp. 28-31, 51.

Carozza, Dick. « *Fighting Fraud With Research* », *Fraud Magazine*, vol. 20, no 5 (2006), pp. 32-36.

Gober, Thomas D. « *Insidious Side Letters: Shady Business on the Side* », Fraud Magazine, vol. 20, no 4 (2006), pp. 25-27, 50.

Holtfreter, Robert E. « *Latest Debit Card Fraud Schemes: Part 1 - Security Breaches Allow Data Thefts* », Fraud Magazine, vol. 20, no 4 (2006), pp. 32-35, 52-53.

Holtfreter, Robert E. « *Latest Debit Card Fraud Schemes: Part 2 - Industry Initiatives, Technology and Global Legislation* », Fraud Magazine, vol. 20, no 5 (2006), pp. 42-43, 50-53.

Lautischer, Pierre E. « *Pension Fraud: Nabbing Bosses Who Crack Nest Eggs* », Fraud Magazine, vol. 21, no 1 (2007), pp. 32-35, 50-51.

Liberti, Francesco. « *Environmental Fraud: More Subtle Than Midnight Dumping* », Fraud Magazine, vol. 20, no 6 (2006), pp. 32-34, 47, 50.

Linn, Courtney J. « *What Asset Forfeiture Teaches us About Providing Restitution in Fraud Cases* », Journal of Money Laundering, vol. 10, no 3 (2007), pp. 215-276.

Luby, Dwayne. « *Pharmacy Fraud: A Clear Prescription Part 1* », Fraud Magazine, vol. 21, no 3 (2007), pp. 24-27, 47.

Luby, Dwayne. « *Pharmacy Fraud: A Clear Prescription Part 2* », Fraud Magazine, vol. 21, no 4 (2007), pp. 20-23, 43-45.

McFadden, Michael. « *Fraud Investigations: A Case Study in Economic Evaluation* », Policing: An International Journal of Police Strategies and Management, vol. 25, no 4 (2002), pp. 752-761.

Poulos, Andrew. « *Illegal I.D.s* », *Law Enforcement Magazine*, vol. 34, no 4 (2007), pp. 104, 106-111.

Svenson, Torleif. « *Global Fraud: Investigating Suspected Fraud in the Middle East* », Fraud Magazine, vol. 20, no 5 (2006), pp. 24-27.

Wanigon, Slemo D. « *Fraud and the Factor of Fear* », *Fraud Magazine*, vol. 20, no 5 (2006), pp. 28-31, 47, 58.

**Sites Web**

Association of Certified Fraud Examiners
http://www.acfe.org

Fraud and Scam Reference
http://www.nettrace.com.au/resource/reference/fraud.htm

Investigator.com
http://www.einvestigator.com/links/insurance_fraud.htm

National Fraud Information Center
http://www.fraud.org

# Le Serious Fraud Office (R.-U.) et la collaboration internationale

**Par David Jones**
**Responsable des communications**
**Serious Fraud Office,**
**Royaume-Uni (R.-U.)**

Le Serious Fraud Office (SFO) du R.-U. est un organisme poursuivant doté d'une capacité d'enquête. Il concentre ses ressources sur les dossiers de fraude les plus importants et les plus complexes; par conséquent, il est bien connu et constamment sous la loupe des médias.

Le SFO, un organisme civil relevant du procureur général, collabore aussi avec la police dans la plupart de ses dossiers. Les forces de police locales affectent des membres à des enquêtes particulières, apportant leur expertise et aidant à procéder aux arrestations et aux perquisitions.

Tous les dossiers de fraude ne nous sont pas confiés ou ne sont pas acceptés : seuls ceux qui sont importants, complexes et qui nécessitent des compétences juridiques, comptables et d'enquête, dans le cadre d'une opération combinée. Nous traitons 63 dossiers qui, réunis, correspondent à une fraude de plus de 2 milliards de livres sterling. (Les fraudes moins vastes, p.ex. douanes et recettes gouvernementales, sont du ressort des autres éléments du système pénal du R.-U.)

Avant d'accepter un dossier, nous déterminons si l'enquête doit être menée par les responsables de la poursuite. Nous évaluons aussi si elle risque de susciter un intérêt national, des inquiétudes chez le public ou d'exiger des pouvoirs spéciaux pour obtenir de l'information et des documents par la contrainte. Si des documents ne sont pas fournis ou si nous croyons qu'ils ont pu être modifiés, nous pouvons demander à un magistrat d'émettre un mandat de perquisition. Le non-respect d'une ordonnance peut entraîner des poursuites et une peine d'emprisonnement.

**Les enquêteurs et les procureurs doivent collaborer dès les premières étapes de l'enquête jusqu'à l'imposition de la peine et, maintenant, jusqu'aux procédures de confiscation.**

Un autre élément important consiste à déterminer si le dossier comporte un important volet international (victimes, preuves ou biens se trouvant dans d'autres pays et devant être retracés). Ceci peut permettre aussi d'établir s'il y a lieu de faire appel à des groupes d'enquête étrangers pour atteindre nos objectifs dans leurs territoires de compétence.

## Enquêtes multidisciplinaires

La conduite de chaque enquête incombe au SFO. Nous désignons un contrôleur des dossiers, un procureur chevronné responsable de gérer le dossier et de former une équipe appropriée pour enquêter sur les allégations en fonction des exigences du dossier et des ressources offertes.

En général, l'équipe comprend des comptables ou des enquêteurs financiers du SFO comme tel, appuyés par des comptables ou des enquêteurs de l'extérieur demandés par des policiers et engagés à contrat. D'autres membres clés sont des spécialistes de l'informatique judiciaire et experts de la TI, qui décodent, examinent et récupèrent les documents informatiques. Avec la police, ils analysent l'information financière, dont les comptes avec autorisation législative, les comptes de gestion et les sorties de fonds. Ils supervisent aussi les perquisitions dans les bureaux et les résidences et, surtout, retracent l'argent. Il peut y avoir d'anciens membres d'une escouade antifraude qui, après leur retraite, deviennent des enquêteurs civils du SFO, apportant l'expertise spéciale acquise dans le passé. Nous consultons aussi des juricomptables de firmes externes.

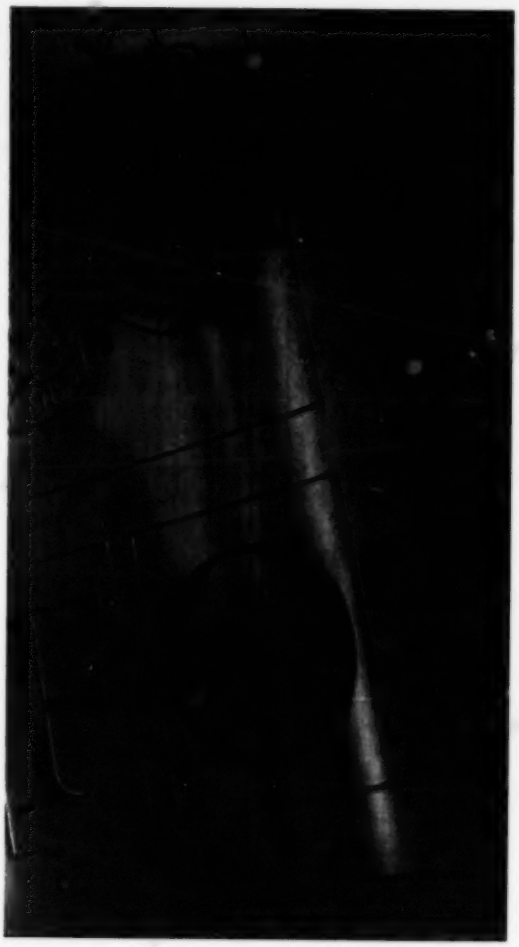
Ce groupe de spécialistes exige une approche d'équipe. Les enquêteurs et les procureurs doivent collaborer dès les premières étapes de l'enquête jusqu'à l'imposition de la peine et, maintenant, jusqu'aux procédures de confiscation.

La fraude a souvent une dimension multijuridictionnelle. Il n'est pas toujours évident de déterminer quelle juridiction doit diriger l'enquête et d'intenter les poursuites

dans chaque dossier. Différentes règles sur les juridictions s'appliquent. En collaborant, nous pouvons transmettre de l'information aux procureurs et aux enquêteurs étrangers durant nos enquêtes. La coordination des recherches est vitale et la collaboration avec plusieurs autres juridictions est excellente.

## Collaboration internationale

Une très grande partie de nos dossiers comprend des éléments de preuve se trouvant à l'étranger. Pour les obtenir, nous devons mener des recherches partout dans le monde, ce qui ne peut être fait qu'en faisant appel aux autorités judiciaires et policières étrangères. De même, les administrations étrangères qui désirent faire des recherches sur des fraudes commises dans leur juridiction et comportant un volet au R.-U. doivent faire appel à nous, que la preuve ou l'intimé se trouve ou non dans notre juridiction. Il s'agit d'une assistance réciproque obtenue par le biais des traités d'entraide juridique et le SFO peut apporter l'expertise de ses enquêteurs afin de permettre à leurs homologues étrangers de mener ces enquêtes au R.-U.



L'aide aux autorités étrangères est fournie essentiellement par le groupe d'entraide juridique du SFO. Celui-ci s'occupe de plus de 50 dossiers, dont certains figurent parmi les plus importants et les plus délicats au niveau international, mettant en cause des personnalités politiques de premier plan, le crime organisé et la corruption à vaste échelle. Le groupe a aidé le gouvernement du Nigeria à retracer des millions de dollars volés par l'ex-président Sani Abacha et sa famille.

Cette forme d'entraide juridique permet de fournir un soutien rapide et efficace à des pays où la corruption et le crime organisé (mafia) causent des problèmes chroniques. Nous avons apporté une assistance à divers pays, dont l'Italie, la Zambie, le Costa Rica, la Russie et le Canada.

En vertu de l'article 2 de la *Criminal Justice Act* du R.-U., des ordonnances obligatoires permettent d'obtenir des éléments de preuve bancaire et d'exiger des réponses à des questions. Nos enquêteurs et avocats travaillent en étroite collaboration avec leurs collègues des pays requérants. Certains pays connaissent peu la loi et l'entraide juridique internationale; nous leur offrons les conseils techniques dont ils ont besoin pour formuler une demande officielle.

La collaboration est réciproque. Sans l'aide des autorités étrangères, plusieurs de nos dossiers n'avanceraient pas. Nos enquêteurs sont des « globe-trotteurs ». Aux niveaux opérationnels officiels et aux niveaux moins officiels, l'assistance transfrontalière est un élément clé de nos processus d'enquête. Nous avons récemment dirigé une série de descentes dans plusieurs établissements en Espagne avec l'entière collaboration et la participation de la police espagnole.

## Relations avec le Canada

En 1997, un citoyen canadien en colère victime d'un stratagème frauduleux de frais d'emprunt payables à l'avance (dirigé par un service fictif de prêts aux entreprises en Angleterre) s'est rendu au R.-U. pour présenter sa plainte. Il avait placé une annonce dans le *Globe and Mail* pour demander si d'autres Canadiens avaient été victimes de cette opération de faux prêts. Plus de 100 personnes ont répondu. Il a apporté la preuve en Angleterre pour en discuter avec la police. Le SFO a par la suite lancé une enquête mettant aussi à contribution deux corps de police britanniques, l'un à Brighton et l'autre à Durham. Nous avons trouvé ultérieurement d'autres victimes de ce stratagème au Canada, aux États-Unis, en Australie et en Nouvelle-Zélande.

Après avoir reçu une demande officielle, la GRC a fourni un soutien tout au long du volet canadien de cette enquête. Lorsque nous avons déployé nos enquêteurs pour recueillir la preuve auprès des victimes, l'un de ces derniers, Ian Wilson, un ancien policier de Durham, se rappelle qu'il venait à peine d'arriver à son hôtel à Toronto lorsqu'un policier de la GRC a demandé à lui parler. De l'avis général, quelques heures ont suffi pour établir un bon niveau de collaboration. L'issue de l'enquête en a été la preuve : les fraudeurs ont été incarcérés.

Le SFO doit avoir une approche pragmatique de ce qui est réalisable. Dans la plupart des cas, les enquêtes sur les fraudes sont difficiles et complexes et, lorsqu'elles sont internationales, elles posent des défis supplémentaires aux enquêteurs. Après près de 20 années d'activités, nous avons acquis une grande expérience de la collaboration avec les groupes antifraude d'autres juridictions. Cerner les criminels internationaux nécessite une collaboration internationale. Nous devons tous utiliser et réviser nos procédures pour que la collaboration soit assurée rapidement. ■

# Saviez-vous que . . .

**Les années du secondaire sont censées être les meilleures années dans la vie des jeunes, mais des incidents violents dans les cours d'école menacent ou compromettent ces années ou y mettent fin brusquement. Les agressions, viols, initiations et autres incidents violents sont une triste réalité pour de nombreux jeunes élèves du secondaire. Voici quelques statistiques.**

Aux États-Unis (É-U.), 22 sur 1 000 élèves âgés de 12 à 18 ans ont été victimes de crimes violents durant l'année scolaire 2004, dont 4 ont été victimes de crimes graves comme le viol, l'agression sexuelle, le vol et les voies de fait graves.

En 2004, 74 % de toutes les agressions commises envers de jeunes Canadiens sur les terrains d'école mettaient en cause le recours à la force physique, 9 %, à des armes (fouets ou véhicules) et 2 %, à des bâtons ou des instruments émoussés.

En France, des écoles secondaires ont signalé 14 780 incidents à la police en 2001-2002 : 34 % mettaient en cause la violence physique non armée, 3 %, l'utilisation de couteaux, et moins de 1 %, des armes à feu.

En 2005, six pour cent des élèves de la 8e à la 12e année ont indiqué qu'ils avaient porté une arme pendant qu'ils se trouvaient sur une propriété scolaire durant les 30 derniers jours.

Dans 71 fusillades survenues dans une école secondaire inscrites dans wikipedia.org depuis 1995, 137 personnes ont été tuées et 232 blessées. L'âge moyen du tireur était de 16 ans.

Aux É.-U., 2 % des écoles publiques ont demandé aux élèves ou aux visiteurs de se soumettre à une inspection à l'aide de détecteurs de métal durant l'année scolaire 2003-2004.

Selon une étude du gouvernement australien, des incidents violents sont plus susceptibles de se produire dans les écoles où plus de 25 % des professeurs ont moins de 5 années d'expérience.

Dans un sondage Phi Delta Kappa sur les attitudes du public à l'égard des écoles ,72 % des participants ont indiqué que la croissance des bandes de jeunes était une cause très importante de violence dans les écoles, la consommation d'alcool et de drogues étant la principale cause.

En 2003, 8 % des cas d'agression sexuelle au Canada contre des jeunes filles de 14 et 17 ans ont eu lieu à l'école.

Selon une étude américaine, plus de 50 % des garçons et 42 % des filles du secondaire croient qu'il est parfois « acceptable qu'un homme ait recours à la force pour avoir une relation sexuelle avec une femme ».

En 2000, 22 % des élèves du secondaire qui ont participé à un sondage mené par l'université Alfred ont dit avoir été soumis à des séances d'initiation dangereuses où ils ont subi de mauvais traitements, été battus, marqués, ligotés, forcés de se blesser ou de blesser d'autres personnes.

Près de trois quart des victimes de séances d'initiation subiront au moins une conséquence négative ultérieure (se battre, blesser quelqu'un, commettre un crime ou envisager de se suicider).

**SOURCES:** *U.S. Department of Justice, Indicators of School Crime and Safety, 2003 : http://www.ojp.usdoj.gov/bjs/abstract/iscs06.htm; Journal of Educational Administration, Vol. 41, No. 6 : http://www.emeraldinsight.com/info/journals/jea/jea.jsp; Statistique Canada, Les enfants et les jeunes victimes de crimes avec violence : http://www.statcan.ca; Wikipedia : www.wikipedia.org; New South Wales Bureau of Crime Statistics and Research, School violence and its antecedents: interviews with high school students : http://www.lawlink.nsw.gov.au; University of Arizona, College of Education : http://www.drugstats.org; North Carolina Coalition Against Sexual Assault : http://www.nccasa.org/teen/GetTheFacts.html; Alfred University : http://www.alfred.edu/hs_hazing*

# Ex-capitale des vols d'auto

## Grâce à la répression efficace des contrevenants actifs à Surrey (C.-B.)

par Carly Paice
de la GRC à Surrey

Jusqu'à tout récemment, Surrey (C.-B.) était connu comme la capitale des vols d'auto en Amérique du Nord – un titre qu'elle s'est acquis en peu de temps, mais qui lui a longtemps collé à la peau. Dans la seule année 2003, on a signalé le vol de 8105 véhicules, une hausse de 120 pour cent par rapport à 1999, ce qui constitue le taux de vol d'autos par habitant parmi les plus élevés au pays.

Entre autres facteurs, l'émergence et l'usage accru de crystal meth est en partie attribuable à cette augmentation aiguë. Si la plupart des véhicules ont été retrouvés (dans un rapport de plus de 90 pour cent), la police était surtout préoccupée par le délai entre le vol et le recouvrement. En effet, ce laps de temps permettait en général aux voleurs de commettre d'autres crimes : vols qualifiés, trafic de drogues, introductions par effraction et conduite dangereuse qui se soldaient souvent par des collisions mortelles ou des blessures graves.

Au printemps 2004, la GRC à Surrey a lancé une initiative de réduction du crime axée sur la répression des vols d'autos et des crimes contre les biens par le repérage des contrevenants les plus actifs. Deux équipes – l'équipe de répression des vols d'auto et l'équipe de répression des crimes contre les biens – ont été mises sur pied afin de cibler le faible pourcentage de contrevenants responsables d'un nombre disproportionné de crimes.

### Stratégies

La nouvelle démarche consistait en partie à nouer de nouveaux partenariats. Sur ce plan, la police a collaboré plus étroitement avec les Services correctionnels du Canada, les services correctionnels et de probation provinciaux, l'équipe municipale et provinciale de répression des vols d'autos (Integrated Municipal Provincial Auto Crime Team, dite IMPACT) et la société de prévention du crime de Surrey (Surrey Crime Prevention Society).

En consultation avec l'avocat de la Couronne, la police a élaboré une matrice incorporant les éléments requis pour une audience de cautionnement. De plus, on a reçu en temps utile toutes les demandes d'information de l'avocat de la Couronne qu'on a relayées sans délai au membre concerné de l'équipe de répression.

La technologie a également joué un rôle déterminant grâce à l'installation de dispositifs de poursuite dans les véhicules volés. Les membres des équipes de répression, entraînés à l'utilisation de ce matériel, ont pu procéder à nombre d'arrestations d'envergure. Les équipes ont également élaboré une démarche plus coordonnée dans la vérification des empreintes des contrevenants en faisant le suivi immédiat de ceux qui présentaient de nombreuses occurrences au fichier.

### Analyse criminelle

Dans le cadre de la stratégie de répression des vols d'auto, le Groupe des analyses criminelles de la GRC à Surrey a été élargi en 2005 et comprend désormais cinq membres. L'analyste en cartographie, chargé de cerner les points chauds et les tendances, ainsi que d'effectuer des analyses prédictives, a joué un rôle déterminant en repérant le lieu où les véhicules étaient volés et abandonnés. Ces données ont permis d'orienter les opérations et le déploiement stratégique des effectifs.

Par exemple, à l'automne 2006, l'analyste en cartographie a cerné une tendance selon laquelle plusieurs véhicules volés de la même marque étaient abandonnés et recouvrés par la police dans un secteur délimité de la ville. Les équipes de répression, redoublant de vigilance dans ce secteur, ont observé un homme torse nu affichant les mots « Grand Theft Auto » (Vol organisé d'autos) tatoués en grosses lettres dans le dos, qui déambulait dans le secteur. Les membres ont vu l'homme voler une voiture de la marque déterminée par l'analyste. L'homme âgé de 27 ans a par la suite été arrêté, fait l'objet d'accusations et mis en détention préventive. Il a plaidé coupable et écopé d'une peine de 26 mois de prison.

Détachement de la GRC à Surrey

L'équipe de ciblage des voleurs d'autos de Surrey a atteint sa cible avec ce suspect au tatouage « Grand Theft Auto » dans le dos. Le suspect a plaidé coupable et a été condamné à 26 mois de prison.

### Résultats

Grâce à la mise sur pied des équipes de répression, à l'élaboration de partenariats et au renfort apporté au Groupe des analyses criminelles, le taux de vols d'autos à Surrey a régressé de 38 % entre 2003 et 2006. En outre, des 737 arrestations et opérations de surveillance réalisées d'avril 2004 à décembre 2006, la totalité des accusations recommandées à la Couronne ont été approuvées, pour un taux de renvoi de 87 pour cent (95 pour cent des affaires se sont soldées par un plaidoyer de culpabilité).

Les membres des équipes de répression des vols d'auto et des crimes contre les biens étaient fiers de recevoir le prix international du mérite pour la répression des vols d'auto, édition 2007, décerné par l'Association internationale des chefs de police à la Nouvelle-Orléans, le 16 octobre 2007. ■

**Grâce à la mise sur pied des équipes de répression, le taux de vols d'autos à Surrey a régressé de 38 % entre 2003 et 2006.**

# RÉVISION DU *POLICE ACT* DE NOUVELLE-ZÉLANDE PAR WIKI

## Pour donner voix au chapitre au public

**par le surint. Hamish McCardle**
**Équipe d'examen du *Police Act***
**Police de Nouvelle-Zélande**

En mars 2006, le gouvernement néo-zélandais s'est engagé à procéder à un examen approfondi des dispositions législatives régissant les services de police au pays, ce qui s'est traduit par la révision du *Police Act* de 1958 (loi sur la police) et du règlement connexe. En tant qu'organisme le plus directement touché par la législation actuelle, et de par sa capacité privilégiée d'en cerner les forces et les lacunes, la Police de Nouvelle-Zélande s'est vu confier le mandat de diriger l'examen.

L'examen de la loi sur la police comporte un vaste mandat, qui reflète le désir d'amorcer un dialogue national avec les citoyens au sujet des services policiers. L'équipe chargée de l'examen a donc été habilitée à revenir sur les principes fondamentaux, à remettre en question les choses tenues pour acquises et à encourager un débat public.

L'équipe a donc décidé d'adopter des méthodes de communication et de consultation à la fois traditionnelles et novatrices afin d'entendre le plus de voix possible. Elle a notamment fait la part belle aux supports en ligne et électroniques dans ce processus.

### Un processus législatif d'avenir

Afin de donner aux Néo-Zélandais voix au chapitre dans l'élaboration de la future loi sur la police, l'équipe d'examen a prévu une consultation publique en trois phases. Dans les deux premières, on a invité les répondants à faire des suggestions concernant une série de documents de discussion. On a notamment élaboré des formulaires en ligne simplifiés permettant aux citoyens de répondre directement aux questions posées dans les documents par voie électronique ou conventionnelle. Dans ces deux phases, la majorité des répondants ont opté pour le mode électronique.

L'élaboration d'un format wiki pour obtenir des idées nouvelles sur la loi sur la police est apparue comme la prochaine étape logique pour recueillir l'opinion non seulement des citoyens au pays, mais également des Néo-Zélandais expatriés et d'autres citoyens à l'étranger intéressés par la police et le processus législatif. Si l'équipe d'examen a jugé relativement utiles les consultations en ligne tenues précédemment, elle estimait qu'une discussion sur wiki permettrait de pousser plus loin la réflexion. L'équipe a préféré tenir un wiki ouvert, sans mot de passe ni modalités d'inscription, afin de faciliter un processus dynamique de suggestions.


Pour faciliter la gestion des discussions, le wiki n'était ouvert aux révisions que durant les heures de bureau du pays. En dehors de ces heures, les gens pouvaient consulter la loi sur wiki et rédiger leurs commentaires hors ligne, pour ensuite les afficher à la prochaine ouverture.

L'équipe d'examen a d'abord inscrit à la loi sur wiki quelques idées pour lancer le processus et fournir un cadre aux collaborateurs. Cela dit, ces derniers ont vite fait d'apporter des modifications en ajoutant des sections nouvelles ou en précisant les éléments qu'ils souhaitaient voir dans la nouvelle loi. Il est devenu évident que de nombreux participants désiraient également discuter de leur ajout ou commenter ceux des autres collaborateurs. La dynamique des discussions était un motif important dans le recours à la technologie wiki, c'est pourquoi l'équipe d'examen a ajouté des pages de notes à chaque article afin de circonscrire les débats à l'extérieur des pages du document principal.

La loi wiki a fait l'objet de près de 26 000 visites, la majeure partie de celles-ci résultant de renvois incorporés à des articles d'actualité en ligne. Comme la plupart des gens visitaient le site par suite d'un renvoi des médias, la répartition des visiteurs semblait refléter l'intérêt des médias pour le sujet, et cet intérêt était d'envergure internationale, surtout par suite d'un article que la BBC a publié à ce sujet sur sa page Web principale.

Des articles en langues étrangères sur la loi wiki ont également paru dans les

médias grand public de nombreux pays : Allemagne, Norvège, Espagne, Hongrie, République tchèque, Thaïlande, Italie, Finlande, Pologne, Malaisie, Chili et France. Une communauté en ligne importante, Slashdot.org, a publicisé l'initiative par suite de l'article de la BBC, ce qui a rapidement décuplé le nombre de visiteurs d'adresses IP américaines (de l'ordre de 7000 pour cent).

On a fermé le wiki le 30 septembre 2007 pour réviser les commentaires, puis on a rouvert le wiki sous forme de document enregistré le 1er octobre. Le site http://wiki.policeact.govt.nz reçoit encore de nombreuses visites au quotidien, et chaque visiteur consulte en moyenne près de quatre pages à la fois. On invite également les gens à communiquer directement avec l'équipe pour lui faire part de leurs commentaires; nous recevons toujours des commentaires à ce jour.

D'après les statistiques, les visiteurs utilisent le wiki du document enregistré de manière différente par rapport à leur utilisation du wiki ouvert initialement. Ils passent plus de temps dans le site et consultent davantage de pages. La proportion des visiteurs accédant au site directement, sans renvoi d'un site média, est également à la hausse.

Étant donné le rayonnement international de l'initiative, les membres de l'équipe d'examen ont été abordés par divers observateurs et chercheurs étrangers souhaitant obtenir plus de renseignements sur le wiki. Nombre de ces derniers ont posé des questions sur les leçons que d'autres services de police pourraient tirer de l'initiative néo-zélandaise.

Le recours au wiki pour l'examen de la loi sur la police a été favorisé du fait qu'il s'harmonisait à l'initiative de gouvernement électronique de la Nouvelle-Zélande, selon laquelle les technologies d'information devraient faire partie intégrante du mode de prestation de l'information, des services et des programmes gouvernementaux. Cette volonté de promouvoir les nouvelles technologies a grandement facilité la mise en oeuvre d'une consultation novatrice et a de toute évidence joué un rôle déterminant dans l'efficacité du wiki.

## Qu'est-ce qu'un wiki?

Inspiré du mot hawaïen wiki wiki, qui signifie rapide, un wiki est une collection de sites web ou d'autres ressources en ligne qui permet aux visiteurs de faire des ajouts, de supprimer ou de réviser un contenu de façon collective. C'est la facilité et la rapidité d'intéraction qui font l'efficacité d'un wiki pour une rédaction collective. Quoique vulnérables aux abus et au vandalisme, les wikis jouissent d'une fonction inhérente d'autocorrection qui tient au nombre d'utilisateurs.

Cela dit, le recours à un wiki dans le processus législatif a initialement été mis en doute, parce qu'il s'agissait d'une méthode inédite, en Nouvelle-Zélande, et dans le monde entier. Les doutes ont cependant été dissipés lorsqu'on a précisé le rôle que le wiki définitif jouerait dans les étapes subséquentes de l'élaboration de politiques. D'autres écueils du wiki étaient plutôt d'ordre pratique – la modération des articles (tel que noté ci-dessus), la gestion des révisions malveillantes et de leurs auteurs – et la maintenance générale du site, entre autres.

### Des résultats éloquents

En gros, le wiki a donné lieu à des centaines de révisions constructives, qu'il s'agisse de suggestions de mots individuels ou de paragraphes étendus de commentaires sur divers aspects. Il a produit au moins trois résultats positifs : d'abord, il a permis de recueillir de nombreuses idées novatrices; ensuite, il a grandement favorisé la sensibilisation et la participation à l'examen et, enfin, bien que ce n'ait pas été un objectif direct de l'examen, l'initiative a suscité un débat approfondi sur l'usage par le gouvernement de technologies axées sur le Web et de sites de réseautage en ligne.

À la lumière de la réussite du wiki ouvert, on a élaboré une deuxième génération de wiki. Ce site, protégé par mot de passe, permet de participer à une initiative visant à raffiner la première génération du wiki de la loi sur la police de 2008. ■

# Enquêtes sur l'exploitation des enfants dans Internet

## Comment surmonter les difficultés émotionnelles

Par Carolyn Burns

En plus d'enquêter sur le viol et la torture d'enfants innocents, les membres des équipes de lutte contre l'exploitation des enfants dans Internet du monde entier sont souvent témoins de ces actes effroyables. Pour reprendre les mots d'un enquêteur, « c'est comme être derrière une vitre et regarder un enfant se faire maltraiter sans pouvoir faire quoi que ce soit pour le protéger ».

Dans le cadre des enquêtes criminelles, les membres des équipes de lutte contre l'exploitation des enfants dans Internet doivent visionner des images explicites d'enfants abusés sexuellement, voire torturés, afin d'identifier les victimes et les suspects et de recueillir des éléments de preuve en vue d'éventuelles poursuites pénales. Il peut s'agir de photographies de jeunes enfants maltraités ou encore de vidéos explicites où l'on voit et entend des bébés torturés et violés. Le temps consacré au visionnement varie, mais il demeure un élément important de l'enquête qui peut laisser des séquelles chez les enquêteurs.

Pour comprendre les répercussions possibles de ces enquêtes et explorer des stratégies qui permettent de s'adapter à ce travail, on a réalisé une étude en collaboration avec l'équipe de lutte contre l'exploitation des enfants dans Internet de la GRC en Colombie-Britannique (C.-B.). À partir de l'expérience des enquêteurs, on a pu dégager des conclusions uniques et importantes relativement aux effets du travail de même que des stratégies auxquelles les enquêteurs ont recours pour surmonter les difficultés associées à leur travail.

### Répercussions du travail

L'expérience personnelle des enquêteurs, les stratégies d'adaptation utilisées et la nature choquante des documents visionnés sont autant de facteurs qui influent sur les répercussions du travail sur les enquêteurs. Il n'est pas rare pour un enquêteur de se sentir dépassé par le volume des enquêtes ou la dépravation et les préjudices dont des enfants et des bébés sont victimes. La société et les membres du système de justice pénale et des services de police sont dépourvus d'une compréhension complète de l'exploitation des enfants, ce qui nuit souvent aux enquêtes et entraîne une vive frustration. Malgré l'importance et la nécessité de leur travail, les enquêteurs ont beaucoup de difficultés à parler de leurs préoccupations à cause du malaise associé à l'exploitation des enfants, ce qui crée chez eux un sentiment d'isolement et de dévalorisation.

Parmi les réactions physiologiques et émotionnelles mentionnées par plusieurs enquêteurs, notons des maux de tête fréquents, des sautes d'humeur et une fatigue extrême qui les empêche souvent de mener leurs activités normales en dehors du travail et leur donne l'impression qu'ils ne peuvent pas remplir leurs engagements envers leur famille et leurs amis.

Les enquêteurs qui voient des images traumatisantes ont souvent des cauchemars, des flashbacks, des pensées envahissantes et de la difficulté à dormir et à se concentrer. L'horreur des images visionnées aggrave le problème puisqu'elle empêche les enquêteurs d'en discuter avec des personnes autres que leurs collègues et les prive d'un exutoire précieux.

De nombreux enquêteurs ont déclaré que ce travail les rendait très protecteurs envers les enfants. Plusieurs ont dit constamment surveiller le comportement des gens côtoyant des enfants. D'autres ont dit avoir absolument besoin de parler à tous les parents et enfants des dangers qui guettent les internautes. Certains, qui ont eux-mêmes des enfants, ont avoué être beaucoup moins permissifs que d'autres parents en raison de toutes les horreurs dont ils sont au courant.

Au cours des trois années d'existence de l'équipe de lutte contre l'exploitation des enfants dans Internet de la C.-B., ses membres ont appris quels sont les éléments qui contribuent ou font obstacle à leur capacité de faire face aux difficultés de leur travail, et ont ensuite créé une série de stratégies. Les stratégies qui suivent sont quelques-unes des techniques utilisées par des membres de l'équipe afin de supporter les images difficiles qu'ils doivent régulièrement visionner.

### Stratégies de visualisation

Les enquêteurs estiment qu'une présentation graduelle des images est préférable pour les nouveaux membres de l'équipe. Ceux qui en ont bénéficié ont déclaré que cela les avait aidés à se préparer à voir des documents de plus en plus choquants.

En outre, la possibilité de se préparer mentalement au visionnement des images aide les membres de l'équipe à affronter ce qu'ils s'apprêtent à voir.

Plusieurs participants à l'étude ont déclaré avoir choisi de changer leur perception des images. Certains font semblant que ce ne sont pas de vrais enfants qui sont maltraités; d'autres répriment leurs émotions pour être plus objectifs. De plus, il est très important pour eux de ne pas regarder la victime dans les yeux ni de l'associer à un enfant qu'ils connaissent.

Plusieurs enquêteurs jugent indispensable d'être à l'écoute de la façon dont ils réagissent aux images. Lorsqu'ils se sentent envahir par l'émotion, il est bon pour eux de prendre une pause, d'aller courir ou de parler avec des collègues.

Lorsqu'on visionne des photos ou des vidéos choquantes, il est essentiel de conserver un esprit d'analyse et de se concentrer sur les éléments de preuve que peuvent contenir les images. En travaillant systématiquement dans cette optique, il est plus facile de demeurer objectif.

Les participants ont également soulevé des facteurs qui influent sur leur capacité de supporter le visionnement de photos et de vidéos choquantes, par exemple, le fait de visionner le matin (il reste ainsi plusieurs heures pour que les images s'effacent avant le retour à la maison), de fixer des limites quotidiennes de visionnement, de faire alterner le visionnement avec d'autres tâches et d'éviter de visionner des images lorsqu'on est fatigué ou émotif. Il est également utile de disposer d'un milieu privé et de collègues avec qui échanger et d'avoir la possibilité de prendre des pauses et de parler après avoir vu des images particulièrement horribles.

### Stratégies personnelles

En plus des techniques utilisées au moment du visionnement, les participants ont décrit un certain nombre de stratégies personnelles qui les aident à faire face à leur travail.

- Avoir des passe-temps pour se changer les idées.
- Faire régulièrement de l'exercice physique, souvent intense.
- Faire du yoga, aller marcher, écouter de la musique.
- Fixer des limites quotidiennes de visionnement.
- Cesser de penser au travail à la fin de la journée.
- Établir des limites personnelles et être à l'écoute pour savoir à quel moment il est temps d'accomplir d'autres tâches
- Connaître ses limites personnelles.

Les membres des équipes de lutte contre l'exploitation des enfants dans Internet peuvent se sentir dépassés et se fixer des buts irréalistes en songeant au nombre d'enfants qui sont maltraités. Ils doivent comprendre qu'ils ne peuvent pas porter sur leurs épaules la responsabilité de tous ces enfants. Pour leur santé, ils doivent savoir qu'ils ne peuvent faire que leur part et s'autoriser à cesser de penser au travail à la fin de la journée.

### Soutien des superviseurs

Selon les membres de l'équipe, l'un des facteurs les plus importants est la compréhension des superviseurs. Lorsqu'ils comprennent les répercussions du travail, ils encouragent les enquêteurs à faire ce qui est nécessaire à leur santé. Tous les participants ont déclaré que la possibilité de prendre du recul, de limiter le visionnement, d'aller courir ou d'aller voir d'autres personnes pour rire ou parler dans les moments difficiles était essentielle à leur bien-être.

Compte tenu de la nature de leur travail et de l'impossibilité de parler des images visionnées pour éviter de traumatiser leurs interlocuteurs, les enquêteurs accordent beaucoup d'importance à leur équipe. Il est très important qu'ils travaillent dans une équipe solide dont les membres collaborent efficacement et peuvent se soutenir mutuellement. Le choix des personnes qui ont les qualités, la stabilité émotionnelle et la capacité nécessaires pour faire ce travail est essentiel au bon fonctionnement de l'équipe entière.

Afin de soutenir les membres des équipes de lutte contre l'exploitation des enfants dans Internet dans leurs enquêtes souvent complexes et difficiles, il est important de leur fournir l'information, les outils et les ressources dont ils ont besoin. ■

Carolyn Burns, M.A., travaille dans le domaine de l'assistance aux victimes depuis 17 ans.

## Désamorçage et inoculation

Les membres de l'équipe de lutte contre l'exploitation des enfants dans Internet de la C.-B. ont maintenant accès à un programme de soutien qui les aide à comprendre et à gérer les aspects émotifs de leur travail.

Le programme d'inoculation et de désamorçage mis au point par le Groupe des sciences du comportement de la GRC en C.-B. est un cours facultatif et confidentiel qui est offert à tous les nouveaux membres de l'équipe de lutte contre l'exploitation des enfants dans Internet et auquel s'ajoutent des séances de suivi tous les six mois.

« On montre aux membres du groupe de courts extraits vidéo d'enfants maltraités, explique Teal Maedel, l'une des psychologues qui a mis le programme sur pied. Ensuite, les membres discutent de leurs pensées, de leurs sentiments et de la partie la plus difficile, celle qu'ils aimeraient oublier. »

« Par la suite, les participants discutent des stratégies qui leur ont permis de supporter la vue des images et les animateurs-formateurs (des psychologues) participent à la discussion au besoin. À la fin de chaque séance, les participants parlent d'un élément utile de leur travail. »

Les séances comportent aussi un volet de sensibilisation, dans le cadre duquel des psychologues de l'extérieur traitent de sujets comme la sexualité, la dynamique familiale, le déni cognitif et les stratégies permettant de surmonter les difficultés du travail d'enquêteur.

Les membres de l'équipe de lutte contre l'exploitation des enfants dans Internet de la C.-B. ont tous formulé des commentaires très positifs sur le cours. Le Groupe des sciences du comportement offre maintenant le programme à d'autres services de police.

*—Caroline Ross*

# Récentes études policières

*Voici des extraits d'études récentes en matière de justice et d'application de la loi. Pour consulter la version intégrale des rapports, veuillez visiter le site indiqué à la fin de chaque résumé.*

## Lignes directrices relatives à l'analyse judiciaire des téléphones cellulaires

par Wayne Jansen et Rick Ayers
National Institute of Standards and Technology (É.-U.)

L'analyse judiciaire des téléphones mobiles est une science qui vise la récupération de preuves numériques d'un téléphone mobile, et ce, dans des conditions rigoureuses à l'aide de méthodes reconnues. Lorsqu'un téléphone cellulaire est découvert dans le cadre d'une enquête, l'enquêteur peut se poser de nombreuses questions : Comment assurer le maintien de l'alimentation? Comment manipuler le téléphone? Comment procéder pour examiner des données éventuellement pertinentes contenues dans l'appareil?

Dans le présent article, nous proposons un guide sur la préservation, l'acquisition, l'examen, l'analyse et le compte rendu de preuves numériques se trouvant dans des téléphones cellulaires, qui sont pertinentes pour les autorités judiciaires, les interventions par suite d'incidents, et d'autres genres d'enquête. Nous nous attarderons principalement sur les caractéristiques des téléphones cellulaires, y compris les téléphones intelligents dotés de fonctions avancées. Nous aborderons également les dispositions à prendre en compte dans le cours d'une enquête sur un incident.

**Les preuves numériques sont intrinsèquement très fragiles, surtout celles que l'on trouve dans les cellulaires. Le contenu d'un téléphone cellulaire peut être affecté, voire perdu chaque fois qu'on l'actionne.**

Notre objectif est double : aider les organismes à établir les politiques et les modalités voulues pour aborder les téléphones cellulaires et préparer les spécialistes judiciaires à composer avec des situations inédites mettant en cause des téléphones cellulaires, le cas échéant. Les organismes pourront s'inspirer de nos lignes directrices pour élaborer leurs capacités d'analyse judiciaire, en consultation avec les conseillers juridiques, les fonctionnaires et les cadres à l'interne.

Le contexte d'application des logiciels d'analyse des téléphones cellulaires est très différent de celui des ordinateurs personnels. Alors que ces derniers sont conçus en tant que systèmes polyvalents, les cellulaires sont des appareils spécialisés qui exécutent un ensemble de fonctions prédéterminées. Les fabricants de cellulaires tendent à privilégier un système d'exploitation exclusif plutôt que les systèmes d'exploitation normalisés qui prévalent pour les ordinateurs personnels.

Les preuves numériques sont intrinsèquement très fragiles, surtout celles que l'on trouve dans les cellulaires. Le contenu d'un téléphone cellulaire peut être affecté, voire perdu chaque fois qu'on l'actionne. À l'amorce d'une enquête, il n'est pas toujours évident que celle-ci se soldera par une poursuite en justice. On risque de passer outre à des preuves importantes, de mal les gérer ou de les détruire par inadvertance, sans se rendre compte de la gravité de l'incident.

Peu importe la nature de l'incident, ce sont les mêmes disciplines qui sont mobilisées : premiers intervenants, enquêteurs, techniciens, examinateurs et analystes judiciaires, responsables des éléments de preuve. Les professionnels, en particulier les premiers intervenants, doivent bien comprendre leur rôle et leur responsabilité à l'égard de l'expertise des téléphones cellulaires, et recevoir la formation voulue sur les outils d'analyse, les politiques, les lignes directrices et les procédures judiciaires.

---

Pour consulter la version intégrale du rapport (publié en mai 2007), visiter le site : ***http://csrc.nist.gov/publications/PubsSPs.html***

## Applications policières de la technologie de la réalité augmentée

par Thomas J. Cowper et Michael E. Buerger

La réalité augmentée (RA) constitue l'une des technologies émergentes les plus puissantes du 21e siècle. Les amateurs de sport sont témoins d'une application populaire de la RA chaque fin de semaine : les grandes chaînes télévisées qui amplifient leurs reportages des joutes de football professionnel en surimposant les lignes jaunes de premier essai sur le terrain. Il s'agit d'une application élémentaire, non interactive de la RA. Une autre forme connue de RA est l'écran de visualisation tête haute (VTH) utilisé par les pilotes de chasse.

Contrairement à la réalité virtuelle, où l'utilisateur est totalement plongé dans un monde virtuel généré par ordinateur, et à la virtualité augmentée, où des objets réels

# Récentes études policières

*Voici des extraits d'études récentes en matière de justice et d'application de la loi. Pour consulter la version intégrale des rapports, veuillez visiter le site indiqué à la fin de chaque résumé.*

## Lignes directrices relatives à l'analyse judiciaire des téléphones cellulaires

par Wayne Jansen et Rick Ayers
National Institute of Standards and Technology (É.-U.)

L'analyse judiciaire des téléphones mobiles est une science qui vise la récupération de preuves numériques d'un téléphone mobile, et ce, dans des conditions rigoureuses à l'aide de méthodes reconnues. Lorsqu'un téléphone cellulaire est découvert dans le cadre d'une enquête, l'enquêteur peut se poser de nombreuses questions : Comment assurer le maintien de l'alimentation? Comment manipuler le téléphone? Comment procéder pour examiner des données éventuellement pertinentes contenues dans l'appareil?

Dans le présent article, nous proposons un guide sur la préservation, l'acquisition, l'examen, l'analyse et le compte rendu de preuves numériques se trouvant dans des téléphones cellulaires, qui sont pertinentes pour les autorités judiciaires, les interventions par suite d'incidents, et d'autres genres d'enquête. Nous nous attarderons principalement sur les caractéristiques des téléphones cellulaires, y compris les téléphones intelligents dotés de fonctions avancées. Nous aborderons également les dispositions à prendre en compte dans le cours d'une enquête sur un incident.

**Les preuves numériques sont intrinsèquement très fragiles, surtout celles que l'on trouve dans les cellulaires. Le contenu d'un téléphone cellulaire peut être affecté, voire perdu chaque fois qu'on l'actionne.**

Notre objectif est double : aider les organismes à établir les politiques et les modalités voulues pour aborder les téléphones cellulaires et préparer les spécialistes judiciaires à composer avec des situations inédites mettant en cause des téléphones cellulaires, le cas échéant. Les organismes pourront s'inspirer de nos lignes directrices pour élaborer leurs capacités d'analyse judiciaire, en consultation avec les conseillers juridiques, les fonctionnaires et les cadres à l'interne.

Le contexte d'application des logiciels d'analyse des téléphones cellulaires est très différent de celui des ordinateurs personnels. Alors que ces derniers sont conçus en tant que systèmes polyvalents, les cellulaires sont des appareils spécialisés qui exécutent un ensemble de fonctions prédéterminées. Les fabricants de cellulaires tendent à privilégier un système d'exploitation exclusif plutôt que les systèmes d'exploitation normalisés qui prévalent pour les ordinateurs personnels.

Les preuves numériques sont intrinsèquement très fragiles, surtout celles que l'on trouve dans les cellulaires. Le contenu d'un téléphone cellulaire peut être affecté, voire perdu chaque fois qu'on l'actionne. À l'amorce d'une enquête, il n'est pas toujours évident que celle-ci se soldera par une poursuite en justice. On risque de passer outre à des preuves importantes, de mal les gérer ou de les détruire par inadvertance, sans se rendre compte de la gravité de l'incident.

Peu importe la nature de l'incident, ce sont les mêmes disciplines qui sont mobilisées : premiers intervenants, enquêteurs, techniciens, examinateurs et analystes judiciaires, responsables des éléments de preuve. Les professionnels, en particulier les premiers intervenants, doivent bien comprendre leur rôle et leur responsabilité à l'égard de l'expertise des téléphones cellulaires, et recevoir la formation voulue sur les outils d'analyse, les politiques, les lignes directrices et les procédures judiciaires.

---

Pour consulter la version intégrale du rapport (publié en mai 2007), visiter le site : ***http://csrc.nist.gov/publications/PubsSPs.html***

## Applications policières de la technologie de la réalité augmentée

par Thomas J. Cowper et Michael E. Buerger

La réalité augmentée (RA) constitue l'une des technologies émergentes les plus puissantes du 21e siècle. Les amateurs de sport sont témoins d'une application populaire de la RA chaque fin de semaine : les grandes chaînes télévisées qui amplifient leurs reportages des joutes de football professionnel en surimposant les lignes jaunes de premier essai sur le terrain. Il s'agit d'une application élémentaire, non interactive de la RA. Une autre forme connue de RA est l'écran de visualisation tête haute (VTH) utilisé par les pilotes de chasse.

Contrairement à la réalité virtuelle, où l'utilisateur est totalement plongé dans un monde virtuel généré par ordinateur, et à la virtualité augmentée, où des objets réels

font partie d'une simulation virtuelle, la RA allie des objets réels et virtuels qu'elle affiche en temps réel à l'intention d'un utilisateur dans un environnement réel de façon à favoriser l'exécution de tâches ou de missions préci s. Grâce à une perception de la situation accrue, l'utilisateur peut en théorie accomplir le travail de trois personnes non dotées de la RA.

La technologie de la RA aura un impact profond sur le travail policier, par les méthodes novatrices qu'elle offre pour la répression du crime et du terrorisme. Par contre, elle offre également aux criminels et aux terroristes de nouvelles possibilités d'exploiter et de perturber la société, et de lui porter préjudice. Pour mieux utiliser cette technologie, les policiers doivent bien en comprendre les capacités et les possibilités qui surgiront dans les décennies à venir.

La présente étude a pour but d'offrir aux policiers un aperçu de la RA. Nous entendons aborder les principes fondamentaux et les composantes de cette technologie, ainsi que les développements actuels qui pourraient améliorer la performance individuelle. Nous présenterons aussi les répercussions de la RA et certaines applications potentielles pour la police.

Voici quelques-unes de ces applications :

- la reconnaissance du visage, de l'empreinte vocale et d'autres données biométriques de criminels connus afin de permettre leur identification instantanée;
- l'intégration de capteurs chimiques, biologiques et d'explosifs afin d'avertir immédiatement les policiers d'une contamination locale et recommander les mesures de protection pertinentes pour eux-mêmes et le public;
- l'affichage tête haute de données à l'intention des agents en autopatrouille et de données sur la gestion de la circulation régionale afin de rendre la conduite plus sûre et plus efficace, surtout dans les poursuites et les interventions rapides;
- des dispositifs optiques avancés offrant des fonctions de zoom et d'imagerie thermique et infrarouge pour la localisation et l'appréhension de criminels en fuite, de survivants de catastrophes enterrés ou dissimulés, ou de personnes portées disparues;
- des dispositifs optiques avancés permettant aux enquêteurs de lire sur les lèvres à de grandes distances dans les situations où des dispositifs d'écoute ne sont pas pratiques;
- la création de scénarios de formation réalistes pour simuler des milieux de travail policier dangereux, en faisant appel à du matériel pratique et à la participation collective des étudiants à la formation;
- la supervision d'interventions dans des incidents critiques axée sur le contrôle de l'état physiologique du personnel, de façon à affecter les tâches dangereuses à ceux qui sont le plus aptes, mentalement et physiquement.

---

Pour consulter la version intégrale du rapport (figurant à la section law enforcement services), visiter le site : ***http://www.fbi.gov/publications.htm***

## Étude nationale sur le recours à la prise d'étranglement chez les policiers

**Par le Centre canadien de recherches policières**

Au Canada (et en Amérique du Nord en général), on assiste à un nombre croissant d'incidents où des policiers affrontent des individus sur lesquels les techniques standard de contrainte restent sans effet. En général, ces personnes sont sous l'emprise de stimulants du système nerveux central ou d'hallucinogènes, qui entravent les méthodes de neutralisation des policiers.

Même compte tenu de l'avancement des technologies moins meurtrières comme les armes à impulsions (TASER) et d'autres dispositifs comme les projectiles d'impact, il est clair qu'en de nombreux cas les policiers doivent connaître et appliquer des techniques de contrainte à mains nues pour neutraliser un individu. La prise d'étranglement vasculaire (PEV) est une de ces techniques dont l'efficacité ne dépend pas de la capacité de l'individu à sentir un stimulus douloureux et à y réagir.

De nombreux services de police canadiens comptent une prise d'étranglement vasculaire dans le cadre des recours à la force. Toutefois, cette forme de contrainte, contrairement aux autres, a fait l'objet d'un examen minutieux du public et des médias. En raison de la controverse entourant le recours aux prises d'étranglement en général, les politiques, les normes de formation et les plans de leçon varient grandement d'un service à l'autre.

L'examen des antécédents juridiques de l'application de la prise d'étranglement dans la police ainsi que de la documentation médicale révèle l'absence d'un consensus chez les professionnels quant au risque associé à cette technique, la technique la plus sûre et le seuil à partir duquel un agent peut légalement appliquer celle-ci. À la lumière de ces disparités, le Centre canadien de recherches policières s'est vu confier le mandat d'examiner les études actuelles relatives aux prises d'étranglement dans le contexte policier.

Notre étude vise à effectuer une évaluation multidisciplinaire de l'application de la prise d'étranglement chez les policiers, en particulier la prise d'étranglement vasculaire. Le rapport définitif fournit un cadre grâce auquel les gestionnaires pourront prendre des décisions éclairées sur ce qui suit :

- l'évaluation du degré actuel de risque associé au recours à la PEV chez les policiers;
- l'autorisation du recours à cette technique;
- l'élaboration d'une politique sur ce recours, y compris sa situation dans le continuum du recours à la force
- l'élaboration d'une politique relative à la formation, à l'accréditation et à la requalification;
- l'élaboration de normes, de plans et de manuels de formation;
- l'élaboration de stratégies de gestion des risques (saisie et analyse de données).

---

Pour consulter la version intégrale du rapport (TR-03-2007), visiter le site : ***http://www.cprc.org/index.cfm?sector=static&page=library***

# La police transfrontalière et le programme Shiprider

**Brad Kieserman**
**Chef, Operations Law Group**
**Quartier général de la United States Coast Guard**

En août et septembre 2007, 50 agents de la Gendarmerie royale du Canada (GRC) et de la United States Coast Guard (USCG) affectés aux opérations à l'appui des équipes intégrées de la police des frontières (EIPF) ont mené un projet pilote qui pourrait modifier la patrouille de la frontière maritime entre le Canada et les États-Unis.

Pendant deux mois, les agents ont patrouillé deux secteurs à bord du même bateau afin de faire respecter les lois canadiennes et américaines pour lesquelles ils avaient été habilités.

Par l'interception de 187 bateaux, les agents ont saisi 214 livres de marihuana, plus de un million de cigarettes de contrebande, six bateaux et 38 000 $ en argent canadien servant à financer des activités de contrebande. Ils ont également effectué plusieurs missions de recherche et de sauvetage et recueilli des renseignements pour les enquêteurs à terre canadiens et américains. Perçu par la plupart des participants comme un projet réussi, le programme Shiprider semble avoir un brillant avenir.

## Pourquoi le programme Shiprider?

Les liens entre le lieu, le crime, les mesures de contrôle et la nationalité sont de plus en plus complexes, surtout à la frontière. Plus que jamais, les crimes et les mesures de contrôle ne sont pas toujours associés à un même pays. Souvent, les criminels se servent des frontières internationales comme obstacles opérationnels pour la police. Le programme Shiprider visait à supprimer la frontière maritime internationale qui nuisait au maintien de l'ordre et à empêcher les contrebandiers et autres criminels à d'exploiter illicitement les eaux communes.

## Comment le programme fonctionne-t-il?

Pour valider le principe, environ 25 agents de chaque pays ont participé pendant près de deux semaines à une formation conjointe en juillet 2007 à la Maritime Law Enforcement Academy de la USCG à Charleston, en Caroline du Sud. Dans le cadre d'un programme spécial élaboré par la GRC, la USCG et le U.S. Immigration and Customs Enforcement (ICE), les agents ont participé à des exposés et à de nombreux exercices pratiques afin de connaître et de comparer leurs tactiques, techniques, procédures et pouvoirs respectifs.

En cohabitant et en travaillant au sein des mêmes équipes binationales comme ils le feraient pour les patrouilles maritimes, les agents ont développé une confiance mutuelle et conclu des partenariats en préparation aux opérations conjointes. À la fin de la formation, chaque agent a été désigné agent de la paix pour l'autre pays, c'est-à-dire que les membres de la GRC ont été désignés agents des douanes américaines et que les agents de la USCG ont été désignés gendarmes surnuméraires de la GRC.

Puis les agents ont été affectés à l'une des deux EIPF, soit Blaine, État de Washington–Vancouver, Colombie-Britannique, ou Cornwall, Ontario–Massena, New York. Après une visite de reconnaissance des lieux, les agents ont commencé les patrouilles quotidiennes à bord des bateaux de la GRC et de la USCG.

Les agents des deux services ont constitué ensemble l'équipage de chacun des bateaux afin que les opérations au Canada soient directement supervisées par un agent de la GRC et que les opérations aux États-Unis soient supervisées directement par un agent de la USCG. Sur les eaux canadiennes, les agents de la USCG aidaient leurs partenaires de la GRC à faire appliquer les lois canadiennes et vice versa. Ainsi, la GRC et la USCG ont supprimé la frontière maritime internationale qui faisait obstacle au maintien de l'ordre et créé un multiplicateur de force : pour le coût d'un seul bateau, les équipes ont patrouillé efficacement les eaux frontalières des deux pays.

USCG

Des agents du programme Shiprider à Cornwall ont saisi ce bateau chargé de 91 caisses de cigarettes de contrebande.

## Comment le programme a-t-il commencé?

Même si protéger la frontière canado-américaine contre la criminalité a toujours été une priorité pour les organismes d'application de la loi et de sécurité publique des deux pays, l'intégrité de la frontière a pris plus d'importance à la suite des attentats terroristes de septembre 2001, moteurs de l'évolution rapide des partenariats entre les deux pays. Au début de 2002, des agents de la GRC et de la USCG s'unissaient pour élaborer des modèles novateurs et efficaces visant à s'assurer que la frontière maritime canado-américaine (4 800 km) allait demeurer ouverte au commerce mais fermée à la criminalité.

En 2003, le commissaire adjoint Mike McDonnell (alors surintendant principal) de la GRC et moi avons eu l'idée d'ajouter un volet maritime aux EIPF. Outre la collecte et l'échange de renseignements, nous avons proposé l'exécution de patrouilles conjointes axées sur les renseignements des eaux de la frontière commune.

En septembre 2005, la GRC et la

USCG ont obtenu l'approbation d'un projet de validation de principe de deux semaines dans la région Windsor-Detroit. Ce projet a donné lieu à une évaluation faisant état des avantages possibles mais soulignant le besoin de plus de formation et d'une plus longue période d'essai. Les deux organismes ont de nouveau testé le programme dans le cadre d'une mesure de sécurité maritime spéciale pour le Super Bown XL en février 2006.

Au terme d'études, d'affectations et d'examens considérables, le commissaire adjoint Raf Souccar de la GRC et le vice-amiral Brian Peterman de la USCG ont proposé aux ministres et aux agents de cabinet, lors du Forum sur la criminalité transfrontalière en novembre 2006, que le concept fasse l'objet d'un projet pilote. En juin 2007, les gouvernements du Canada et des États-Unis ont donné le feu vert au projet en s'appuyant sur la recherche juridique et politique effectuée par les organismes compétents des deux pays. Les surintendants Blair McKnight et Joe Oliver à Ottawa ont fait équipe avec leurs homologues de la USCG, du ICE et de Customs and Border Protection (CBP) pour la mise en oeuvre d'un projet pilote efficace sur les Grands Lacs et la côte ouest.

Suivant le modèle de répression criminelle axée sur les renseignements des EIPF, la GRC et la USCG ont créé un centre conjoint des opérations au détachement de la GRC à Cornwall, où une EIPF bien rodée existait déjà. Profitant de la participation et de la contribution de tous les partenaires EIPF, l'équipe du programme Shiprider à Cornwall-Massena a relevé de nombreux défis posés par la nature multi-juridictionnelle du territoire autochtone chevauchant la frontière canado-américaine dans ce secteur. Souvent, les criminels se livrent à leurs activités dans le territoire adjacent puis retournent dans leur territoire par les voies navigables, croyant ainsi échapper à la détection. Au dire des agents du programme Shiprider, la surprise était sur les visages des premiers contrebandiers fuyant par la frontière, qui ont rencontré un bateau de la USCG avec à son bord des agents de la GRC qui continuaient à les poursuivre au-delà de la frontière maritime!

## Quels sont les autres avantages?

Le programme Shiprider favorise l'intégration des agents d'application de la loi terrestres et maritimes, ce qui est particulièrement important en raison du déplacement ou de la réapparition des activités criminelles dus à la répression exercée inégalement dans la région.

À Cornwall-Massena, la présence accrue d'agents du programme Shiprider sur les voies navigables a repoussé une bonne part des activités de contrebande vers les ponts et les ports d'entrée, où les partenaires EIPF, fin prêts, ont effectué un nombre accru de saisies de contrebande dans les environs.

Selon les évaluateurs, les activités du programme ont amélioré l'intégrité de la frontière. Par sa présence visible, sur l'eau et sur terre, le programme empêche directement les activités criminelles maritimes, soit par la perturbation des voies empruntées par les criminels ou la cessation temporaire des activités de ceux-ci. L'équipe de Colombie-Britannique-Washington a profité de sa présence accrue sur les voies navigables pour faire appliquer les règlements sur la sécurité nautique et les petits bâtiments dans les régions où les patrouilles n'étaient pas régulières.

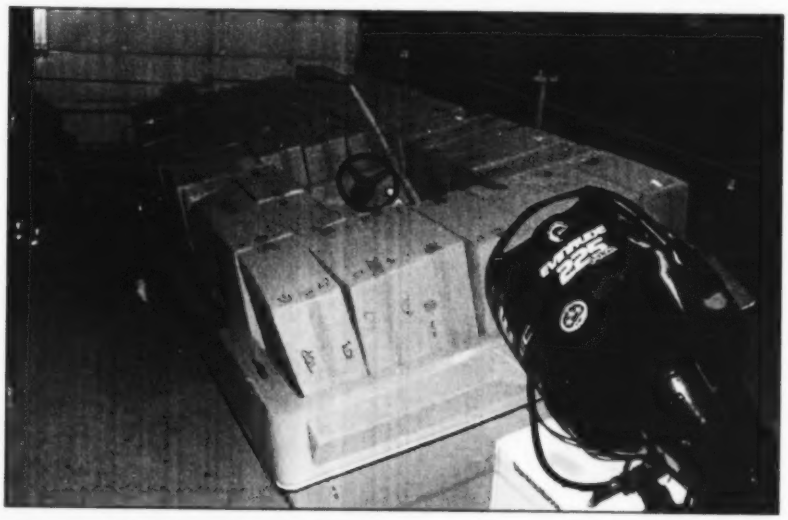
## Prochaines étapes

Sécuritaire et fructueux, le projet pilote de deux mois s'est terminé à la fin de septembre 2007. La GRC et la USCG sont en voie de faire approuver par leur gouvernement respectif l'établissement d'équipes Shiprider à temps plein sur les côtes Est et Ouest ainsi que sur la voie maritime des Grands Lacs et du Saint-Laurent. Les deux organismes croient que les négociations d'un traité officiel sur la mise en oeuvre d'un cadre de travail bilatéral officiel pour la viabilité des opérations du programme Shiprider commenceront au début de 2008.

La GRC et la USCG entendent peaufiner leur programme de formation et offrir le programme Shiprider à d'autres organismes policiers canadiens et américains ayant une capacité maritime.

Partout dans le monde, les services de police savent de plus en plus ce que font leurs homologues d'autres pays. Pour ce qui est de la frontière maritime entre le Canada et les États-Unis, les agents du programme Shiprider des deux pays, en plus de savoir ce que font leurs homologues, travaillent avec eux afin de prévenir l'utilisation de la frontière canado-américaine par les criminels. ■

Les équipes terrestres et maritimes du programme Shiprider ont saisi plus de 200 livres de marihuana le 26 septembre 2007.



USCG

# La radicalisation et le Programme d'approche communautaire de la GRC

**Par l'insp. Wayne Hanniman et Angus Smith**
**Enquêtes criminelles relatives à la sécurité nationale**

Ces dernières années, au Canada comme à l'étranger, plusieurs affaires – dont le Projet OSage (une enquête dirigée par la GRC dans la lutte contre le terrorisme, qui a permis l'arrestation de 17 suspects en 2006), les attentats à la bombe de Londres du 7 juillet 2005 et l'assassinat du cinéaste néerlandais Theo Van Gogh en 2004 – ont prouvé que la menace extrémiste ne vient pas toujours de l'extérieur.

En effet, des citoyens natifs du Canada, des États- Unis, de la Grande-Bretagne, des Pays-Bas et d'une foule d'autres pays répondent à l'appel du radicalisme et de l'extrémisme violent et sont prêts à s'engager dans l'action terroriste.

Les groupes à risque peuvent se composer d'enfants d'immigrés qui se sentent coincés entre les valeurs traditionnelles de leurs parents et le mode de vie trépidant et souvent contradictoire de la société occidentale moderne.

Les agents de la radicalisation peuvent être des chefs religieux ou des idéologues politiques qui profitent de la colère ou de la stupeur de leurs recrues face à des événements internationaux, à des politiques étrangères et à la souffrance des membres de leur communauté religieuse ou de leur groupe culturel dans d'autres régions du monde. De nombreux individus se radicalisent aussi d'eux-mêmes, seuls ou en petits groupes.

Si l'on associe souvent la radicalisation aux communautés musulmanes, il n'y a en fait aucun groupe culturel ou religieux qui soit plus enclin ou plus vulnérable qu'un autre au phénomène. Les adeptes de l'islam ne présentent pas de risque particulier à cet égard. La vaste majorité d'entre eux ne soutiennent pas la cause terroriste et ne commettront jamais d'actes terroristes.

Depuis toujours, les groupes violents de toutes sortes usent des mêmes stratégies pour recruter leurs membres, et ce, parmi le même genre de personnes : des jeunes gens particulièrement vulnérables et impressionnables. Depuis une cinquantaine d'années, les services de police et les organismes de sécurité ont eu maille à partir avec une grande variété de groupes et d'individus radicalisés au point d'entrer dans l'action terroriste : le FLQ et les Squamish Five au Canada; les Weather Underground et les Black Panthers aux États-Unis; le groupe Baader-Meinhof, les Brigades rouges et Action directe en Europe.

## Sensibilisation communautaire

Le Programme de la sécurité nationale en matière d'approche communautaire (PSNAC) est l'un des principaux outils mis en oeuvre par la GRC à l'échelle nationale pour lutter contre la menace posée par la radicalisation. Correspondant parfaitement aux valeurs d'impartialité et de police communautaire de la GRC, à sa priorité stratégique sur la jeunesse et à celle de lutte contre le terrorisme, l'approche communautaire est un élément clé du Programme de la sécurité nationale de la GRC.

Depuis 2005, il existe un Programme d'approche des jeunes qui s'inscrit dans le programme national mais qui est centré sur la radicalisation et la violence liées à l'idéologie politique chez les jeunes, l'objectif étant de faire participer de jeunes adultes au dialogue sur la sécurité nationale et les questions du maintien de l'ordre.

Le Programme d'approche communautaire a été mis en place pour répondre aux préoccupations exprimées par des communautés minoritaires lors de différentes audiences publiques, en particulier celles de la commission d'enquête O'Connor et de l'examen de la *Loi antiterroriste*. Les membres de ces communautés se sentaient marginalisés ou considérés comme des terroristes à cause de leur race ou de leur culture. Ils craignaient de devenir la cible de représailles dans un courant d'opinion anti-minorités que provoquerait un attentat terroriste d'envergure.

Le but du Programme est de mobiliser les diverses communautés ethniques, culturelles et religieuses du Canada pour qu'elles participent à la protection de la sécurité nationale, d'encourager la compréhension des préoccupations et objectifs communs et de favoriser les communications éclairées et pertinentes en temps de crise.

Pour établir une bonne communication entre la GRC et certaines communautés, on organise des rencontres un peu partout au pays. Ces rencontres consistent à expliquer le rôle de la GRC et les responsabilités de l'organisation en matière de sécurité nationale ainsi qu'à entendre les participants discuter ouvertement de leurs préoccupations communautaires.

En temps de crise, des membres du Programme d'approche communautaire et de l'Équipe intégrée de la sécurité nationale (EISN) rencontrent les représentants des communautés touchées pour discuter de l'enquête et de leurs préoccupations concernant d'éventuelles retombées pour la communauté.

À cause de l'incroyable diversité de la population qui bénéficie des services de la GRC, il est indispensable que les programmes qui ciblent des communautés ou des groupes à l'intérieur de ces communautés soient d'une réelle souplesse. Ainsi, le Programme d'approche communautaire a été adapté selon les besoins des régions. À Toronto, les enquêteurs de l'EISN de la Division O ont conçu une série de cours qui connaissent un franc succès. En peu de temps, ces cours donnent aux citoyens un aperçu des principales procédures de police ainsi que des dispositions habilitantes qui en sont le fondement. L'EISN de la Division E a créé l'équivalent à l'intention des jeunes.

Le Programme d'approche communautaire de la GRC est un exemple supplémentaire du travail qu'accomplit la GRC en collaboration avec les communautés ou leurs représentants pour aider des individus ou des groupes à risque à trouver leur place au sein de la société canadienne, sans avoir à renier leurs valeurs culturelles et religieuses. ■